97TH CONGRESS
2d Session

SENATE

REPORT
No. 97-664

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

REPORT

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

MADE BY THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

NOVEMBER 15, 1982.—Ordered to be printed

Filed, under authority of the order of the Senate of OCTOBER 2 (legislative day, SEPTEMBER 8), 1982

U.S. GOVERNMENT PRINTING OFFICE

11-010 O WASHINGTON: 1982

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, Jr., Delaware, *Chairman*

CHARLES H. PERCY, Illinois	THOMAS F. EAGLETON, Missouri
TED STEVENS, Alaska	HENRY M. JACKSON, Washington
CHARLES McC. MATHIAS, Jr., Maryland	LAWTON CHILES, Florida
JOHN C. DANFORTH, Missouri	SAM NUNN, Georgia
WILLIAM S. COHEN, Maine	JOHN GLENN, Ohio
DAVID DURENBERGER, Minnesota	JIM SASSER, Tennessee
MACK MATTINGLY, Georgia	DAVID PRYOR, Arkansas
WARREN RUDMAN, New Hampshire	CARL LEVIN, Michigan
HARRISON "JACK" SCHMITT, New Mexico	

JOAN M. McENTEE, *Staff Director*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

WILLIAM V. ROTH, Jr., Delaware, *Chairman*
WARREN RUDMAN, New Hampshire, *Vice Chairman*

CHARLES H. PERCY, Illinois	SAM NUNN, Georgia
CHARLES McC. MATHIAS, Jr., Maryland	HENRY M. JACKSON, Washington
JOHN C. DANFORTH, Missouri	LAWTON, CHILES, Florida
WILLIAM S. COHEN, Maine	JOHN GLENN, Ohio
	JIM SASSER, Tennessee

S. CASS WEILAND, *Chief Counsel*
ELEANORE J. HILL, *Chief Counsel to the Minority*
KATHERINE BIDDEN, *Chief Clerk*

CONTENTS

	Page
I. Introduction	1
II. Intelligence agencies assessed technology transfer problem	3
CIA report cited Soviet acquisitions	3
Soviets said to have increased desire for U.S. data	5
III. Examples of how Soviets obtain American technology	9
U.S.S.R. exploits six basic techniques to acquire data	9
Case No. 1: How Soviets equipped semi-conductor plant with U.S. machinery	12
Case No. 2: Richard Mueller tried to retain U.S. consultant for Soviets	13
Case No. 3: Mueller and Volker Nast were part of another export combine	15
Case No. 4: Volker Nast tried to export MSR-903 to Hungary	17
Case No. 5: Swarovski was caught with F-4 fighter gunsight camera	18
Case No. 6: Polish spies compromised radar expert William Holden Bell	20
Case No. 7: Marc Andre DeGeyter sought valuable computer code	23
Case No. 8: Walter Spawr sold laser mirrors to the Soviet Union	25
A view from inside the Silicon Valley	25
Case No 9: $3.4 million theft at monolithic memories	29
Case No. 10: Stolen Intel equipment found in Munich	29
Case No. 11: Silicon Valley firm owned by alleged bloc spy	30
A view from inside the Soviet Union	31
IV. Staff recommendations on commerce and national security agencies	35
Remedies proposed in both aspects of preliminary staff inquiry	35
Commerce Department enforces Export Administration Act	35
Recommendation was made to place enforcement in Customs Service	36
Lawrence Brady disagrees with staff recommendation	40
Improvements said to be needed in role of Defense and Intelligence Agencies	41
Recommendations to the Defense Department	42
Recommendations to Intelligence Agencies	43
V. IG report corroborated much of subcommittee staff critique	45
VI. Witnesses offered recommendations to improve export control capability	49
Customs Commissioner opposed enlarging compliance division	49
Shift in enforcement strategy was proposed by computer businessmen	51
FBI embarked on business education program	52
Freedom of Information Act causes problems for Defense Department	54
Buckley and Bryen stressed need to enlist assistance from allies	56
VII. Findings, conclusions and recommendations for corrective action	59
Additional views of Senator William S. Cohen	68

97TH CONGRESS 2d Session | SENATE | REPORT No. 97-664

TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS

NOVEMBER 15, 1982.—Ordered to be printed

Filed, under authority of the order of the Senate of OCTOBER 2 (legislative day, SEPTEMBER 8), 1982

Mr. Roth, from the Committee on Governmental Affairs, submitted the following

REPORT

together with

ADDITIONAL VIEWS

I. INTRODUCTION

The Senate Permanent Subcommittee on Investigations held public hearings in May of 1982 on the ability of the executive branch to enforce export controls, particularly with regard to the transfer of high technology to the Soviet Union and Soviet Bloc.

The hearings, held on May 4, 5, 6, 11, and 12, were based on a preliminary investigation by the subcommittee's minority staff under the direction of Senator Sam Nunn of Georgia, the Ranking Minority Member, and with the concurrence of Senator William V. Roth, Jr., of Delaware, the Chairman. The subcommittee received complete cooperation and vital assistance in its preparation for the hearings from the Senate Intelligence Committee under the guidance of its Chairman, Senator Goldwater and its Ranking Minority Member, Senator Moynihan.

The central point of the investigation and hearings was that the Soviet Union and its satellite states rely on the United States and the Western World for sufficient quantities of high technology equipment to support their military and industrial needs.

The subcommittee's intention was to evaluate the effectiveness of the executive branch in preventing and delaying the flow of technology to the Soviet Bloc; and to recommend legislation and other corrective action to improve export control efforts.

The Federal statutes most affected by technology transfer are the Export Administration Act (50 U.S.C. App. 2401 et seq.); the Arms Export Control Act (22 U.S.C. 2751 et seq.); and the espionage statutes (18 US.C. 792–799).

The Export Administration Act is administered by the Commerce Department and has to do with the export of unclassified equipment and technology. Under this category is so-called dual-use technology; that is, technology which has both civilian and military applications.

Information developed in the investigation indicated that the Soviet Union has made the acquisition of United States dual-use technology an important priority. The ability of the Commerce Department to enforce export controls on dual-use technology was a principal interest of the subcommittee in the investigation and hearings.

In addition, the subcommittee examined the efficiency and effectiveness of the executive branch in obtaining and utilizing intelligence information concerning the Soviet Union's Western technology acquisition program. Also examined was coordination among the Departments of State, Defense, Justice, and Commerce, the U.S. Customs Service and other agencies in shaping and executing export control policy.

The investigation and hearings were held under authority of Senate Resolution 361 of March 5, 1980, and 333 of March 4, 1982, in which the Senate Permanent Subcommittee on Investigations of the Governmental Affairs Committee was authorized to examine the efficiency and economy of all government operations, including those functions affecting national security.

In the 5 days of hearings, 24 witnesses testified in 643 pages of stenographic testimony in connection with 37 exhibits.

II. Intelligence Agencies Assessed Technology Transfer Problem

Subcommittee inquiry led to CIA report on Soviet acquisition

Early in its inquiry, the Senate Permanent Subcommittee on Investigations, coordinating its efforts with the Select Committee on Intelligence, asked the Central Intelligence Agency for assistance in evaluating the success of the Soviet Union's programs to acquire Western technology.

The CIA, in March of 1981, began to assemble information on military gains the Soviets have registered in obtaining Western technology. According to Admiral Bobby R. Inman, Deputy Director of the CIA, the study took 6 months to complete and its results were "startling to those of us inside the intelligence community".

Testifying before the Investigations Subcommittee, Admiral Inman said the report, "Soviet Acquisition of Western Technology," was first submitted to the Senate Intelligence Committee and was then made available in unclassified form to the Investigations Subcommittee and the public. The sanitized version of the report, dated April 1982, was received as Exhibit No. 1 at the subcommittee hearings.

The CIA report pointed to striking similarities between the U.S. Minuteman silo and the Soviet SS–13 silo, the SS–13 being the first Soviet solid propellant ICBM. Acquisition of Western ballistic missile guidance and control technology enhanced the latest generation of Soviet ICBMs, the CIA report said.

The improved accuracy of the Soviet ICBMs stemmed from the acquisition from the West of gyroscopes, accelerometers and other guidance components the U.S.S.R. could not have developed on its own in so short a time. The CIA report said the ability to manufacture another essential ingredient in ICBM technology—small, precision, high-speed bearings—was achieved in part, by the Soviets in the 1970's through legal trade purchases from the West.

In aircraft technology, the Soviets obtained hardware and data from planes downed or captured in Vietnam, but the U.S.S.R. has remained in constant pursuit of the most advanced aircraft technologies from the West. The CIA report said Soviet military aircraft designers have been able to obtain specifications on the American C–5A transport and other Western airplanes. U.S. military transports and wide-body jets have been used as models by the Soviets. The Soviets' IL–86 looks much like the Boeing 747 and the IL–76 Candid resembles the C–141, although neither system is an identical copy.

The CIA report said the Soviet Union's new advanced early warning and control aircraft, the Tupolev TU–126—"Moss," which is expected to be operational by the mid-1980s, is strikingly similar to the American AWACS (Airborne Warning and Control System).

In Naval acquisitions, the Soviets bought two huge floating drydocks from the West ostensibly for civilian purposes but the drydocks, essential for repair of ships damaged in warfare, were diverted to

military use—one to the Soviets' Pacific Naval Fleet in 1978, the other to the Northern Fleet in 1981. The drydocks, capable of servicing the new Kiev-class V/STOL aircraft carriers, are so large and complex that no Soviet shipyard was sufficiently large or equipped to build them. The drydocks' importance will grow when they will be needed for the larger Soviet carriers planned to be operational in the 1990s.

The CIA report added:

> The Soviets even have acquired Western aircraft carrier catapult equipment and documentation for this larger carrier; catapult technology, though relatively common in the West, is outside the Soviet experience.

The Soviets, who have the world's largest oceanographic fleet, modernized their ships with Western-manufactured equipment and will use this technology to help support the development of weapons systems programs for anti-submarine systems against the West, the CIA report said.

In those tactical weapons areas where the Soviet Union has serious technical deficiencies—such as in developing smart weapons, electro-optical and signal and information-processing technologies—it has strengthened its military position by Western acquisitions. More often, however, Western technology is used to speed up a developmental program or to improve upon original Western designs promptly, the CIA report said, pointing out that:

> The Soviets appear to have concentrated their tactical systems acquisitions on Western tank, anti-tank and air defense-related technology and equipment in order to derive concepts and know-how to benefit their weapons programs and to design countermeasures to the Western systems.

The report noted that the Soviet SA–7 heat-seeking, shoulder-fired anti-aircraft missile contains many features of the U.S. Redeye missile.

In microelectronics, Western equipment and know-how have added to the Soviet Union's production capabilities. The CIA report said:

> These acquisitions have permitted the Soviets to systematically build a modern microelectronics industry which will be the critical basis for enhancing the sophistication of future Soviet military systems for decades. The acquired equipment and know-how, if combined, could meet 100 percent of the Soviets' high-quality microelectronic needs for military purposes, or 50 percent of all their microelectronic needs.

The Soviet Bloc's Ryad computers, used in a wide variety of military and civil applications, are patterned after the IBM 360 and 370 series. By using Western models such as these, the Soviets and East Europeans were able to develop and produce general purpose computers in a risk-free environment, saving time, manpower and money.

In summary, the CIA report said, by acquiring Western technology, the Soviets saved hundreds of millions of dollars in research and development costs, modernized their military industry, limited production costs, achieved improved weapons performance and incorporated countermeasures to Western weapons early in the development of their own weapons programs.

The CIA report said that, in terms of financial gains and losses, the West has lost more from sales to the Soviets than it has gained; that is, if the West pursues the costly objective of trying to keep pace with Soviet military gains. The report explained:

> . . . it is clear that the Western military expenditures needed to overcome or defend against the military capabilities derived by the acquisition of Western technology far outweigh the West's earnings from the legal sales to the Soviets of its equipment and technology.

SOVIETS SAID TO HAVE INCREASED DESIRE FOR U.S. DATA

Dr. Jack Vorona, whose Defense Intelligence Agency technology transfer office made an important contribution to the CIA's Soviet acquisition report, testified that the U.S.S.R. today is devoting more resources than ever before to the task of obtaining and exploiting American technical expertise and equipment.

Dr. Vorona, Assistant Director of Scientific Intelligence at the DIA, said the Soviets' primary target in the United States is dual-use technologies; that is, technology having both military and civilian applications. He pointed out that Soviet military uses of American know-how far outweigh civilian applications in the U.S.S.R. So dominant a role does American technology play in the Soviets' military and industrial scheme that it is likely that they have come to think of U.S. research and development programs as their own. Dr. Vorona explained:

> . . . the U.S. R&D establishment is viewed by the Soviets as a Mother Lode of important and frequently openly available (science and technology) information. In fact, they tap into it so frequently that one must wonder if they regard U.S. R&D as their own national asset. They have enjoyed great success in this endeavor with minimal effort, primarily because, as a nation, we lack the awareness of what they are about.

Dr. Vorona said the Soviets use every method imaginable to obtain American technology—studying U.S. open literature, setting up Communist-owned firms in the United States and elsewhere, bribing or blackmailing persons with sensitive information and exploiting student and scientific exchange programs. Of the Soviet Academy of Sciences, Dr. Vorona said:

> There should be no doubt that this prestigious academic organization is a key and witting participant which, via such mechanisms as scientific and student exchanges, contributes significantly to the total take.

Dr. Vorona traced the history of the Soviets in technology acquisition since World War II. He said that the Soviet's impressive radar capabilities of today have their origin in American Lend-Lease equipment. This machinery, coupled with information the Soviets obtained from a Massachusetts Institute of Technology Radiation Laboratory

publication on radar theory, provided the building blocks upon which the Soviets began their radar design programs.

Crediting the Soviets with being "excellent radar theorists" and having made many contributions on their own, Dr. Vorona noted that the acquisition of American microcircuitry enabled the Soviets to reduce the weight and size of their radar sets so that they could use them on board military aircraft. The Soviets' "Look Down/Shoot Down" interceptor, the modified Foxbat, reflects the application of embargoed U.S. microelectronics, Dr. Vorona said, observing that William Holden Bell, the Hughes Aircraft radar expert who sold Polish spies military secrets, may have enhanced significantly Soviet radar technology. Of the Bell case, Dr. Vorona said:

> . . . we haven't begun to see the repercussions. . . . The classified data transmitted is no doubt right now being investigated to further Soviet radar capabilities and countermeasure our own.[1]

Dr. Vorona said the Soviet chemical warfare capability came from Germany after World War II; their TU–4 Bomber was a direct copy of the U.S. B–29; the Soviets' first jet engine, used on their Mig-15 fighter aircraft, was from Rolls Royce; a scientist brought in from Germany after the war taught the Soviets how to produce fissionable material; and secret information provided by British physicist Klaus Fuchs was an important factor in enabling the Soviets to produce nuclear weapons.

American intelligence analysts mistakenly assumed that the Soviets' post-World War II Western acquisition programs were temporary, that they would decline as the Russians pumped more and more of their own resources into R&D program. But the decline never occurred, Dr. Vorona said. The Soviets apparently have no intention of reducing their reliance on Western technology.

By using Western technology, Dr. Vorona said, the Soviets and their satellite states have saved hundreds of millions of dollars in R&D costs and years in development time. Their acquisition program enables them to avoid the element of risk in developing new concepts. An added bonus they receive is a close working knowledge of the state of U.S. weaponry, giving them the opportunity to construct countermeasures to new U.S. weapons before they are deployed.

In the immediate future, Dr. Vorona said, the U.S. can expect the Soviets to be seeking components for their electronics, aerospace and shipbuilding industries. These acquisition efforts are likely to focus on American defense contractors, general producers of military-related auxiliary manufacturing equipment and small and medium-sized firms and research centers that develop advanced component technology and design. Small firms will be "specially enticing" for the Soviets because many of these enterprises are on the cutting edge of important technological breakthroughs. Yet because they are starting out, their products have not yet been incorporated into military programs and "are thus unclassified and vulnerable."

---

[1] William Holden Bell, in Federal prison for espionage, was a witness before the subcommittee. A summary of his testimony begins on p. 20 of this report.

Not everyone agrees with the American intelligence community's assessment of the threat to national security posed by Soviet acquisition of U.S. technology. Reflective of the disagreement was an editorial from the New York Times of April 12, 1982 in which the newspaper said that lowering the barriers to the flow of technology to the U.S.S.R. is not necessarily a bad thing. The Times editorial said:

> A more relaxed policy would serve the West's best interests because a steady supply of foreign technology saps the Soviet Union's incentives to develop its own. It is better to have the Soviets stealing, copying and following a few steps behind than working independently in becoming able to deliver a technological surprise.

Asked to respond to the editorial, CIA Deputy Director Bobby Inman called the editorial "wishful dreaming." Dr. Vorona said the editorial was "divorced from reality." Dr. Vorona went on to say:

> The Soviets are bent upon achieving world preeminence, dominance, if you will, in science and technology and are building a huge R&D infrastructure with that goal in mind. The technology they are acquiring from the West is an important input to that process because it allows them to compare and build upon the best of both worlds and they do.
>
> A more relaxed export policy, rather than condemning them to second place, as the editorial seems to imply, would only hasten their achieving world class status.

Dr. Vorona also said:

> . . . the Soviet leadership appreciates and has often times noted the causal relation between science and technology and strategic superiority. To them, technology transfer is an important means to that end.

INTENTIONAL
BLANK

III. Examples of How Soviets Obtain American Technology

U.S.S.R. EXPLOITS SIX BASIC TECHNIQUES TO ACQUIRE DATA

Dr. Lara H. Baker, Jr., an internationally known computer scientist employed by the Los Alamos, New Mexico Laboratory of the Department of Energy, described for the subcommittee six basic techniques the Soviets use to obtain U.S. technology.

Dr. Baker, who serves as a consultant on technical matters to the American intelligence community and the armed services, referred first to the traditional "hand-in-the-safe" information-gathering crafts as practiced by the Soviet spy organizations, such as the KGB and the GRU,[1] whose tactics include bribery, blackmail and extortion in their attempts to obtain American military secrets and non-classified but militarily critical technology. Dr. Baker explained:

> These traditional methods are used primarily to obtain high-priority technology that cannot be obtained through less risky techniques. The effectiveness of these methods is shown by the amount of effort the Soviets put into them and by the amount of priority they give these activities. Such traditional theft methods are most effective at obtaining technology that is considered most sensitive by our side.

Frequently, Russian spies pose as diplomats. For example, in 1979 and 1980, Marc Andre DeGeyter, a Belgian with financial ties to the U.S.S.R., tried to obtain by bribery a multi-million dollar source code for the Soviets from a Northern Virginia computer firm. When FBI agents arrested DeGeyter, a Soviet diplomat, Georgiy V. Veremey, contacted the same computer company to obtain information about the same source code. The DeGeyter case is described in detail later in this report.

Dr. Baker said the second vehicle the Soviets rely on in technology transfer is information published by the U.S. Government and made available to the public by Federal agencies. Similarly, the Soviets promptly translate into Russian U.S. technical journals and distribute them among their scientists and engineers, Dr. Baker said:

> We live in a free society and are proud of that fact. One of our greatest strengths is the information transfer that our Constitution allows and that we encourage among our own people. Tapping into this information flow is an extremely fruitful technique for the Soviets to use. The U.S. Government is the focus for much of the information flow on sensitive, high technology items. Through use of the U.S. Government repositories set up to handle unclassified documents and through use of the Freedom of Information Act to retrieve formerly classified or currently classified documents, foreign

[1] The KGB is the Soviet Committee for State Security. The GRU is the Chief Intelligence Directorate of the Soviet General Staff.

agents have been able to acquire information of significant strategic value.

Also of high importance is the fact that they have been able to tie up a significant quantity of U.S. Government resources. These resources are dedicated to answering Freedom of Information Act requests, checking for downgrading and classification of documents, and evaluating national security implications of documents. Many U.S. Government agencies have had to set up offices to handle these requests and divert highly competent people from analysis activities to evaluation of FOIA requests, some from foreign nationals.

In our society, one of the most treasured freedoms is free speech. This reaches its epitome on the freedom of organizations to produce periodicals covering whatever they wish to talk about. As a result, magazines in this country, such as Aviation Week and Space Technology, carry a large quantity of information of particular defense interest. While these publications do serve an extremely useful purpose in keeping the defense community informed about the complex activities going on in the Free World, they also provide a conduit for information to the Soviets. Information suggests the Soviets place a very high priority on Western technical journals, including providing translations in near real time with publication. In many cases, the information available in these journals is of higher quality than that available in government documents.

The third tactic is for the Soviets to promote student exchanges as ways to improve relations between the United States and the Soviet Union. Dr. Baker said these exchange programs were created as part of the spirit of détente. However, he said:

> This was a particular coup on the part of the Soviets, since the best technology transfer organization in the world is the United States university system. In the U.S. universities, a very large number of highly qualified, highly motivated, superbly trained people spend their working lives trying to come up with better ways to transfer technology to their students. These people are called university professors. It's their job, and they do it very well.

Dr. Baker said that about one-half the graduate students in the United States are not U.S. citizens. The non-U.S. fraction for many science and engineering programs is higher. He said projections indicate that by 1985 at some universities, such as the University of California at Berkeley, up to 90 percent of the graduate students may not be U.S. citizens.

While there are government restrictions on Soviet participation in graduate programs, Dr. Baker said, these restrictions are not applied as stringently to Soviet Bloc students. He said information that is transferred to the Soviet Bloc is immediately made available to the Soviet Union. Thus, the U.S. graduate schools help "alleviate the Soviet problems with training really first-rate engineers." Dr. Baker said.

In the electrical engineering programs at the Massachusetts Institute of Technology, Stanford University and several other institutions, a student can enroll in a one-year curriculum in microprocessor chip technology.[3] Explaining the significance of what such programs mean in terms of technology transfer, Dr. Baker said:

> During that year, the student will have used computer-aided design to design the microprocessor, he will have used computer-aided layout to lay out the processor on silicon, manufactured the chip either in the laboratory or in collaboration with a manufacturer, tested the circuit, packaged the circuit, mounted the microcomputer on a printed circuit board, and made the resulting computer work. Thus, in one year, the student will have been exposed to an intense, carefully orchestrated program covering the United States integrated circuit industry. This would have been done under the supervision of experts, with careful hand-holding throughout the program to make sure that the student understood his activities. Fortunately, evidence indicates that the number of foreign students who have gone through these programs so far is minimal.

A fourth device employed by the Soviets and their satellite states is to form marketing and manufacturing companies in the U.S. whose purposes are two-fold—to buy high technology and munitions for illicit export to the Soviet Union; and to serve as havens for spies. Dr. Baker said the tangled web of ownership of many U.S. corporations obscured the identity of their true owners. He said Eastern Bloc or Soviet corporations can be recipients of U.S. technology without the donors of that technology realizing that the information is going to a foreign government. "This kind of foreign ownership of U.S. corporations presents a potential serious hazard," Dr. Baker said.

In the William Holden Bell case, which will be discussed later in this report, Polish spies controlled a firm in Chicago known as Polamco, for Polish American Company. Using Polamco as a base of operations, they bribed Bell, a Hughes Aircraft radar expert, and were able to obtain from him valuable military secrets.

The fifth category of Soviet strategy to obtain U.S. technology is to rely on agreements providing for scientific exchanges. Dr. Baker said that as part of détente the U.S. entered into bilateral agreements with the Soviet Union on scientific and technical subjects, including atomic energy. As part of these agreements, the U.S. furnished technical information and equipment.

Pointing out that in these agreements the U.S. found itself giving up more than it got back, Dr. Baker cited one such pact in which the United States loaned the Soviets a multi-million dollar magnet "in return for intangibles."

Sixth—and one of the Soviets' most successful acquisition devices—has been the use of business intermediaries, companies established in the United States, Western Europe and elsewhere which buy high technology of American origin and then ship it to the Soviet Bloc. Dr. Baker said an example of the Soviets' use of business intermediaries was seen in the CTC-Maluta case.

---

[3] A microprocessor is a computer on one integrated circuit.

The subcommittee's minority staff devoted considerable resources to reconstructing the activities of the CTC-Maluta syndicate of business intermediaries. This network of companies, controlled from West Germany, was instrumental in giving the Soviets the technology to make a major leap forward in modernizing their military electronics capability. Dr. Baker, who had personal knowledge of the CTC-Maluta case, was one of the subcommittee's sources in reconstructing the activities of the network. Other sources included the Departments of Commerce and Justice and the U.S. Customs Service.

CASE NO. 1: HOW SOVIETS EQUIPPED SEMI-CONDUCTOR PLANT WITH U.S. MACHINERY

The CTC-Maluta case came about when a syndicate of electronics companies was set up in Western Europe and Southern California by a 34-year-old West German named Werner J. Bruchhausen. Several of Bruchhausen's Southern California enterprises had the initials CTC and all were managed by his principal American accomplice, Anatoli Maluta, also known as Tony Metz, a Russian-born naturalized American citizen.

Using Bruchhausen's companies and accomplices in Western Europe as freight forwarders and transshipment points, Maluta sent more than $10 million in American-made high technology equipment to the Soviet Union from 1977 to 1980. Much of the machinery was used to equip a Soviet plant for the manufacture and testing of semi-conductors.[4] The equipment went from California to Western Europe to the U.S.S.R.

To Dr. Baker, the CTC-Maluta case proved his point that the Soviets know precisely what U.S. technology they want; they leave little to chance, Dr. Baker said, explaining:

> Of particular interest to me in the (CTC-Maluta) case is the information it gives us about Soviet intentions. We delude ourselves if we think the Soviets enter the black market in search of strategic components in a helter-skelter style, buying up dual-use commodities without rhyme or reason.
>
> The truth of the matter is that the Soviets and their surrogates buy nothing they don't have specific, well defined needs for. They know exactly what they want—right down to the model number—and what they want is part of a carefully crafted design.

The carefully crafted design in this instance, Dr. Baker said, was the semi-conductor manufacturing plant, an essential part of the Soviets' desire to close the technological gap between themselves and the U.S. in the integrated circuit/microcomputer industry.

Dr. Baker, who testified in the 1981 successful prosecution of Maluta and his associate, Sabina Dorn Tittel, said he studied 400 separate air waybills and other shipping documents used by the CTC network. He said the conclusion was inescapable that the Soviets were equipping a

[4] Semiconductors are the class of materials used as the basis for most modern electronic components. Such materials are called semiconductors because they have electrical properties between conductors (e.g., copper) and insulators (e.g., glass). An integrated circuit is a single piece of semiconductor (usually Silicon) containing several components (transistors, resistors, etc.) integrated into a single functional electrical circuit.

semi-conductor plant. He said the Soviets' use of components of U.S. origin demonstrated their determination to make the facility as efficient and modern as any in the world. He explained:

> . . . (the Soviets) have purchased clandestinely all the hardware they need for equipping a good integrated circuit production plant. They showed no interest in purchasing production equipment that was not state of the art. They showed very good taste.

Stressing his point that, through the CTC-Maluta combine, the Soviets bought everything they needed for a semi-conductor manufacturing plant, Dr. Baker testified that among the equipment they bought over the period 1977 through 1980 were saws for cutting silicon crystals, equipment for making masks for integrated circuit production, plotters to draw the circuits, basic computer-aided design systems for integrated circuit design, diffusion ovens for circuit production, ion-implantation systems for circuit production, photo-lithographic systems for integrated circuit production, scribers for separating integrated circuits on wafers, testers for testing integrated circuits on wafers, bonding equipment for bonding connecting leads to integrated circuits, and packaging equipment for packaging the circuits. Dr. Baker went on to say:

> High quality integrated circuits are the basis of modern military electronics. Integrated circuits form the basis for military systems which are more flexible, more capable and more reliable than systems using discrete electronic components. The production tooling and equipment obtained by the Soviets (from the CTC-Maluta network) will significantly improve the Soviets' capability to produce such circuits.

CASE NO. 2: RICHARD MUELLER TRIED TO RETAIN U.S. CONSULTANT FOR SOVIETS

Further support for the assertion that the Soviets relied on American technology for equipping of their semi-conductor plant came from John D. Marshall, a chemist and specialist in the operation of facilities that manufacture semi-conductors.

Marshall, who owns a high technology business in that section of Santa Clara County, California known as the Silicon Valley, testified that in the winter of 1975 he made two trips to the Soviet Union.

Led by a West German named Richard Mueller to believe that the Soviets wanted to retain his consultative services in connection with their plans to manufacture electronic watches, Marshall learned on his second trip to Moscow that what was actually desired of him was his expertise in equipping a semi-conductor plant. Marshall told the subcommittee:

> On the second trip, we met several Soviets who purported to be technical people. They were not very well trained and were not familiar with sophisticated technological thinking. But it was apparent to me by the questions they asked and the subjects they discussed that the Soviets had built a semi-

> conductor manufacturing and assembly plant and they were anxious to equip it.
>
> They wanted American semi-conductor manufacturing equipment and they had detailed literature on the precise kind of equipment they wanted. They also wanted me to obtain for them certain semi-conductor components.
>
> It was clear to me that Mueller had deceived me as to the Soviets' intentions, that it was not merely electronic watches the Soviets wanted to manufacture.

Marshall said he realized that for him to cooperate any further with the Soviets would have constituted questionable or illegal conduct on his part. He said he refused to meet further with the Soviets and left Moscow.

As he returned to the United States, Marshall began to recall recent conversations he had overheard that at the time had not made sense to him but now were becoming clear. Traveling to Moscow, for example, Marshall and Mueller had stopped over in Hamburg where Mueller introduced him to a Canadian, whose name he could not remember, who made remarks to the effect that he also was providing technical assistance to the Soviets, that his mission was to show them how to make integrated circuits and how to use properly equipment they soon would be obtaining.

In Moscow, Marshall said, he met a women who spoke English with a German accent who was planning to ship certain American-made photo-lithography materials to the Soviet Union via East Berlin. Photo-lithography materials are critical in semi-conductor manufacture. Marshall could not remember the woman's name.

In West Germany, Marshall was introduced to a man namel Volker Nast, identified by Mueller as being his partner. As will be shown in this report, Nast was deeply involved in illegal diversions of U.S. technology to the Soviet Union.

The significance of 1975 as being the year in which the Soviets expressed their desire for American-made semi-conductor equipment was explained by Marshall. He said in 1975 the U.S. was pre-eminent in the field of semi-conductor technology. He said:

> It is my view that the Soviets had built their manufacturing plant, or plants, to specifications for American-made equipment—for the manufacture, assembly and testing of integrated circuits. Now that the facilities were constructed, they were, in the winter of 1975, confronted with the next step, which was to equip the facilities.

Marshall said that the Soviets' primary interest in equipment in 1975 related to the manufacture and assembly phases of semi-conductor production. By 1977, he said, the Soviets would have been ready to stock the facility with the test equipment; and with software development equipment.

Dr. Lara Baker, in his testimony before the subcommittee, said his knowledge of the sequence of events in the purchase of the semi-conductor equipment squared with Marshall's. In the 1978–1979 time frame. Dr. Baker said, the CTC-Maluta syndicate was purchasing production equipment. In the 1979–1980 period, the CTC-Maluta network was buying semi-conductor test equipment. Marshall's testimony "is quite consistent with my information," Dr. Baker said.

CASE NO. 3: MUELLER AND VOLKER NAST WERE PART OF ANOTHER EXPORT COMBINE

Additional information about the Soviets' efforts to build their own semiconductor industry—and, in so doing, make a major leap forward in military electronics—was given the subcommittee by Charles L. McLeod, a Special Agent with the U.S. Customs Service. McLeod said the same Richard Mueller who had brought John Marshall to Moscow had been active in several other schemes to assist the Soviets.

In fact, McLeod said, Mueller was an operative in a syndicate whose mission was to export by illegal means semi-conductor manufacturing equipment from the United States to the Soviet Union. Other operatives in the network included Volker Nast, Luther Heidecke, Peter Gessner and Frederick Linnhoff, all West Germans. In the U.S., their accomplices included Robert C. Johnson, Gerald R. Starek and Carl E. Storey, officers of high technology firms.

McLeod, assigned to the San Francisco office of Customs where he investigated technology diversions originating in nearby Santa Clara County, said his inquiries into two Silicon Valley electronics firms—II Industries and Kaspar Electronics—led him to the conclusion that the Soviets were trying in the mid-1970's to "construct a semi-conductor manufacturing facility by using U.S. technology and equipment."

In a subcommittee affidavit, received as Exhibit No. 31 at the hearings, McLeod said a loosely knit organization of electronics producers and brokers in West Germany and Northern California assisted the Soviets in realizing their ambitions in the semi-conductor field.

The first diversion of semi-conductor manufacturing equipment he told the subcommittee about occurred in 1974. McLeod said participants in the diversion included Luther Heidecke, a representative of Honeywell/West Germany, AG, and Peter Gessner, the European sales representative for Applied Materials, a Northern California business which produced semi-conductor manufacturing equipment. Gessner had other jobs as well, serving as the European salesman for II Industries and Kaspar Electronics. In addition, Gessner was employed by Richard Mueller.

Processing orders through Honeywell/West Germany for the purchase of semiconductor manufacturing equipment, Heidecke arranged for the export of II Industries and Kaspar Electronics machinery to West Germany and ultimately to the Soviet Union, McLeod said, adding that Heidecke's activities were brought to the attention of the West German authorities, who prosecuted him for giving the Soviets national security information.

McLeod described a second diversion. A Mays Landing, New Jersey export firm known as a Semi-Con, formed by the West German Richard Mueller and managed by a former intelligence agent, was alleged to be shipping semiconductor manufacturing equipment to the Soviet Union. The equipment reportedly was from II Industries and Kaspar Electronics.

After investigators from the Commerce Department looked into the allegation by making telephone inquiries to Kaspar and II Industries officials, a full law enforcement investigation was begun in July of 1975 with Customs Service and Justice Department participation. McLeod said examination of business records indicated that semi-conductor

manufacturing equipment originally destined for Semi-Con in Mays Landing was, in fact, actually shipped to two Montreal firms, USA Trade and Semitronics.

McLeod said the shipper's documentation showed the end-user to be Canadians but the electrical power usage on the equipment itself had been converted to adapt to European voltage standards, evidence that Canada served only as a transshipment point in the movement of the freight to another destination.

In September of 1975, McLeod said, Customs agents developed information indicating that Robert C. Johnson, president of Kaspar Electronics, and two II Industries officers—Gerald Starek and Carl Storey—were conspiring with Richard Mueller to ship semi-conductor equipment to the Soviet Union in violation of the Export Administration Act.

Referring to Mueller as a West German businessman who operated two businesses there, Techmex and Semitronic, McLeod went on to say:

> Mueller was no stranger to U.S. authorities. He had previously been implicated in 1974 (when) he was involved in the illegal diversion of high technology equipment to the Soviet Union by Honeywell, AG of West Germany.

Mueller suspected the authorities might detect his use of Semi-Con of Mays Landings as the forwarder of the semi-conductor equipment to West Europe for transshipment to the Soviet Union. McLeod thought the telephone calls to II Industries and Kaspar Electronics from Commerce Department investigators might have caused Mueller's concern. So, McLeod said, Mueller, in league with Johnson, Starek and Storey, rerouted the shipment through Montreal since validated export licenses are not required under the Export Administration Act for exports of nonclassified high technology to Canada.

Cooperating with U.S. Customs, the Royal Canadian Mounted Police learned that the two Montreal firms, USA Trade and Semitronics, were companies in name only and that the true destination of the shipment had been a Montreal freight forwarder, Kuhn & Nagel, which, upon receipt of the cargo, had transshipped it to Switzerland. There the II Industries and Kaspar Electronics cargo was received by Semitronics of Zurich. The freight was forwarded on to the Soviet Union.

Customs Special Agent McLeod cited two other illegal high technology diversions involving II Industries and Kaspar Electronics, both of which were routed from Northern California through Kansas to Hamburg, Germany and then on to the Soviet Union. The first shipment got through without detection by U.S. Customs. The second was intercepted in Kansas City by Customs agents. They removed the semiconductor manufacturing equipment from the crate and replaced it with sand. Then, while the cargo was still in Kansas City, Frederick Linnhoff, a West German national working as an accomplice of Richard Mueller and Volker Nast, was allowed by authorities to forward the freight to Hamburg where it was received by a "Reimer Klimatechnik," a pseudonym used by Nast. West German Customs agents picked up the surveillance of the sandbox. Later Linnhoff informed the German police that Nast had told him the bogus shipment did make it through to Moscow.

McLeod said Johnson of Kaspar Electronics and Starek and Storey of II Industries were convicted of violations of the Export Administration Act but did not serve prison terms. McLeod said Richard Mueller, Volker Nast and Linnhoff were indicted but returned to Germany and are fugitives from American justice.

Summing up his investigative experience in regard to the II Industries-Kaspar Electronics diversions, McLeod said:

> It is my personal observation that the Soviet Union lacks advanced technology relating to the semi-conductor manufacturing industry. During the past 6 to 8 years, there has been evidence which illustrates that the Soviets have made great efforts, at a great expense, to obtain any and all technology relating to semi-conductor manufacturing.

CASE NO. 4: VOLKER NAST TRIED TO EXPORT MSR-903 TO HUNGARY

Volker Nast, Richard Mueller's partner, was the instigator of an attempt in the summer of 1980 to export to the Soviet Bloc nation of Hungary by illegal means a Microwave Surveillance Receiver system, the MSR-903, manufactured by the Micro-Tel Corporation of Baltimore. Designed to receive, display and analyze microwave signals, the MSR-903 is a highly sophisticated system whose primary uses are military and whose export is controlled by the Department of State under the Arms Export Control Act.

According to Michael Dolphin, Special Agent of the U.S. Customs Service, Volker Nast enlisted the aid of another West German, Rolf Peter Herms, and a Princeton, New Jersey man, Werner Richard Hilpert, in his effort to obtain the MSR-903

Dolphin, whose subcommittee affidavit was received as Exhibit No. 30 at the hearings, said the Customs Service learned that Herms had written to Hilpert asking him to purchase the MSR-903 from Micro-Tel.

Informed by Micro-Tel officials that he would need a license from the State Department if he wanted to export the MSR-903, Hilpert assured them that someone else was obtaining the necessary clearances. Hilpert made a $10,000 downpayment on the $47,000 system.

Dolphin said that in January of 1981, Hilpert's wife and Rolf Peter Herms went to Micro-Tel offices, paid the $37,000 balance owed and left with the MSR-903, which was about the size of a large suitcase and weighed about 78 pounds. A Customs surveillance team, which included 18 agents and had the use of a helicopter and a court-authorized electronic "beeper" hidden inside the MSR-903, followed Herms and Mrs. Hilpert as they drove from Baltimore to the Hilperts' home in New Jersey.

The next morning, Mrs. Hilpert and Herms drove to New York City. Herms, carrying the MSR-903, left Mrs. Hilpert and took a taxi to the John F. Kennedy International Airport where he checked all his luggage at the Pan American ticket counter. At that point, Customs Agents arrested Herms and took possession of the MSR-903, Dolphin said.

Confronted with evidence of his guilt, Herms admitted he was working for Volker Nast. Nast, who already was a fugitive from American justice in connection with his indictment in the II Industries-Kaspar

Electronics prosecution, was charged in a two-count indictment by a Federal grand jury in Baltimore for conspiracy to violate the Arms Export Control Act. Nast remains a fugitive at this writing. Herms was given a 2-year suspended sentence and 5 years' probation and allowed to return to West Germany. Werner Hilpert was given 3 years of probation and fined $10,000, Dolphin said.

CASE NO. 5 : SWAROVSKI WAS CAUGHT WITH F-4 FIGHTER GUNSIGHT CAMERA

Manfred Swarovski, a member of a wealthy and influential Austrian family, owned and operated an optical equipment company in his homeland. He set up two businesses in North America—Swarolite of Canada, Ltd., located in Moose Jaw, Saskatchewan; and Swarolite, Inc., of Columbia, Tennessee.

John Rennish, a Special Agent of the U.S. Customs Service, said that Swarovski came to the attention of Federal investigators in the spring of 1975 when he placed an order with Photo-Sonics of Burbank, California to buy a special gunsight camera, model KB25A, used on the U.S. Air Force F-4 fighter aircraft.

Keeping the Customs Service informed of all his dealings with Swarovski, John Kiel, president of Photo-Sonics, believed that Swarovski intended to take the gunsight camera to Canada and then ship it to Austria. Customs Agent Rennish, who gave the subcommittee this account in an affidavit received as Exhibit No. 29 in the hearings, said Photo-Sonics was told by investigators to follow Swarovski's instructions and to ship the gunsight camera to the Swarolite facility in Columbia, Tennessee. Rennish said Customs agents made certain that Swarovski was advised formally and in writing that export of the gunsight camera was illegal unless first licensed by the State Department under the Arms Export Control Act.

The gunsight camera, mailed to Columbia in care of Swarolite, was delivered to a motel on the outskirts of town where Swarovski was staying. Rennish said Customs agents began surveillance of Swarovski.

Swarovski flew by commercial aircraft to Chicago where he went shopping and dined in a restaurant. He boarded a flight to New York where he registered at the Waldorf Astoria Hotel and, according to Rennish, "seemed to be enjoying himself considerably, shopping, dining out, frequenting several bars and entertaining women friends in his room."

Rennish, who was in charge of the 15 member Customs surveillance team, said that while at the Waldorf Astoria Swarovski tried to disguise himself, changing his hair style, assuming a different manner of dress and wearing sunglasses.

After 2 days in New York, Swarovski went to the John F. Kennedy International Airport where he confirmed his reservation on a Pan American flight to Munich. He checked his luggage at the Pan Am counter and went to the predeparture lounge to wait for his flight.

Rennish said that Customs agents, operating under Federal law (22 U.S.C. 401) which gives them the right to search luggage under these circumstances, went through Swarovski's suitcases and found the gunsight camera. Rennish placed Swarovski under arrest and had his rights read to him in English and German. Several business cards of Soviet officials were found in a search of Swarovski's person.

The Swarovski case was one of several cases the subcommittee examined which demonstrated the complexity of conducting export control inquiries and the constraints within which agents must work. Rennish said:

> The export violation occurred, according to the U.S. District Courts' interpretation of the law, at that moment when Swarovski checked his luggage through to Munich at the Pan Am ticket counter in the JFK Airport terminal. We believed that Swarovski intended to take the camera into Austria and there have his freight forwarder ship the camera to a destination in the Soviet Union. If we could have had access to official shipping documents in Austria, we could have tried to demonstrate that he planned to transfer the camera to the Soviet Bloc. Unfortunately, however, because U.S. Customs agents received very little cooperation from the Austrian government, we were not able to document or otherwise establish that Swarovski intended to ship the camera from Austria to the Soviet Bloc. Austria, a neutral country which shares borders with the Soviet Bloc nations of Hungary, Yugoslavia and Czechoslovakia, was not supportive of Customs' investigative efforts.

Rennish said that records of Swarolite of Canada were given to U.S. Customs by a cooperating co-conspirator. The records revealed that on previous occasions Swarovski had bought American high technology equipment with military applications and sought to export it to an Austrian freight forwarder without licenses. But, because Austrian officials would not assist them, U.S. Customs agents could not document the fact that the items were actually shipped to the Soviet Bloc. Rennish said Customs agents were able to show that Swarovski had tried but failed to buy from the National Aeronautics and Space Administration a NASA moon-mapping lens.

Rennish added:

> The lack of cooperation in the Swarovski inquiry from Austria was not unique to this case. U.S. Customs receives poor cooperation from Austria in many export violations. Another neutral European nation, Switzerland, does not make a great effort to help in export violations in many cases.

Citing a deficiency in Federal law, Rennish said there is no "attempt" provision in the current export control statutes. Because of that deficiency, he said, the violator can be apprehended only after he actually does the act of exporting. In Swarovski's case, the act of violating the law occurred at the moment he checked his luggage containing the gunsight camera. Rennish explained:

> It was then that he presented his merchandise for export. This requirement means that surveillance must be continuous on a suspect until that moment when he violates the law. The cost of such surveillance can be prohibitive if it goes on too long. Consider, for example, that instead of staying only 2 days in New York City he had stayed 2 months or longer. At some point, Customs might have been forced to curtail the inquiry and hope to detect him at the airport. But any number

of things can go wrong once the surveillance is stopped. Swarovski could have rented a car and driven to Boston or Newark and flown abroad from there. The slightest change in plans could have resulted in his escaping Customs and successfully carrying the camera out of the country.

Citing another deficiency in Federal law, Rennish pointed out that in enforcing export laws Customs agents do not have the authority to arrest without a warrant.

> They can investigate, search and seize but there is no statutory authority under the export laws to arrest. Arrests can be made if they are in States where Customs agents are deemed to be peace officers of that State. Customs agents have no State peace officer certification in New York. Swarovski's arrest by Customs agents was only one aspect of the inquiry that Swarovski's attorney challenged in court.
>
> The attorney, Richard Kuh, instituted suppression arguments and appeals which lasted in court hearings for the next 26 months. Swarovski's search, seizure and arrest were attacked. Ultimately, the suppression and appeals hearings proved unsuccessful. But the arrest issue went all the way to the Supreme Court where it was upheld as a citizen's arrest. His appeals exhausted, Swarovski pleaded guilty and served a 2-year sentence.

Rennish quoted the judge in Swarovski's trial, George C. Pratt of the U.S. District Court in the Eastern District of New York, who noted the difficulties U.S. Customs agents must work under in export cases. Citing the fact that export laws give Customs agents the right to seize and search in connection with munitions violations, but not to arrest, Judge Pratt said:

> The fault, if there be any, lies with Congress which has failed to grant Customs officers statutory authority to make arrests under the Munitions Control Act. Congress passed the act with broad powers of search and seizure, and commanded the Secretary of the Treasury to enforce it. Congress did not, however, take the additional step and grant to the Customs agents specific statutory authority similar to that granted to them to apprehend narcotics and revenue violators. As a result, Customs agents are powerless to arrest on the scene those persons who are caught in an attempt to illegally export under the Munitions Control Act.

Rennish added that the lack of statutory authority to make a warrantless arrest described by Judge Pratt is still a restriction that Customs agents must work under in export violations.

CASE NO. 6: POLISH SPIES COMPROMISED RADAR EXPERT WILLIAM HOLDEN BELL

The subcommittee examined the William Holden Bell-Marian Zacharski case as an instance in which Soviet Bloc spies, working out of a Polish-owned company in the United States, cultivated and then compromised an American defense industry engineer and obtained from him significant amounts of secret military information.

Burdened with debts and back taxes, family tragedy and a job with no future, William Holden Bell needed a friend. Bell, a 60-year-old Hughes Aircraft radar engineer, found such a companion in 30-year-old Marian Zacharski, who lived near Bell and his young Belgian wife Rita in the Cross Creek Village apartment complex in Playa del Rey in Los Angeles County.

Testifying before the subcommittee, Bell said he knew Zacharski to be a Polish national and the West Coast manager of the Polish-owned machine manufacturing firm, Polamco, incorporated in Delaware and Illinois and with offices in Chicago, Detroit, and Los Angeles. But, Bell said, he was not concerned about a national security problem in his association with Zacharski, believing that Soviet Bloc spies sought to inject themselves into the lives of defense industry engineers like himself only in Europe and other foreign places. "When you are sent to Europe, you are told to expect attempts by foreign spies," Bell testified, "but whoever expected it to happen here at home?"

Bell and Zacharski played tennis on a daily basis. With their wives, they met socially. Zacharski "slowly became my best friend," Bell recalled, noting also that the Polish manufacturing executive had a liberal expense account and used it generously. Bell said Zacharski asked him to make a few contacts for Polamco sales. Bell did and, without advance notice, Zacharski paid him $4,000. In addition, Zacharski told Bell he might be needed as a consultant for Polamco once he retired from Hughes.

Looking toward future employment with Polamco, Bell said, he tried to demonstrate to Zacharski his own professional competence and showed him a document he had prepared at Hughes Aircraft on a sensitive military subject. Bell said the document was classified secret and that, though he gave it to Zacharski on the tennis court, his Polish friend took it home to read.

At this stage of his relationship with Zacharski, Bell said, he justified his own conduct on the theory that Polamco was just like any other industrial company in the United States which used gratuities and other forms of payoffs to obtain company secrets from competitors. Bell explained:

> An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to their security classification. He may also be asked to provide specific documents directly. Sometimes the engineer is hired. More often he is not. This is generally tolerated because, of course, both companies are American. And they are in competition with each other.

Bell's initial perception of Zacharski as just another foreign business executive was enhanced, he said, by the fact that Zacharski, by virtue of his Polamco credentials, had access to government facilities, such as atomic energy installations and Naval shipyards.

Under the pretense of helping Bell buy his apartment in the complex that was being converted into a condominium, Zacharski began giving cash payments to the Hughes engineer. Bell testified:

> In view of my prospective employment by Polamco, he (Zacharski) thought he could help me. Subsequently, he appeared at my door handing me envelopes of cash. With this money I made the downpayment on the condominium and paid the Internal Revenue Service. I signed a receipt for the money and concealed the source from my wife.

Bell began photographing sensitive documents he brought home from Hughes. He went to Innsbruck, Austria and met with more Polish agents. His expenses on this trip and three others—to Innsbruck again, to Lintz and to Geneva—were paid by Zacharski. The agents were not guessing about Bell's worth to them, Bell said, explaining:

> They knew exactly what they wanted, right down to the company identification numbers.

Before he was arrested by the Federal Bureau of Investigation, Bell had received a total of $110,000 over the 3-year period from 1977 to 1980. The CIA report of April of 1982 entitled, "Soviet Acquisition of Western Technology," received as Exhibit No. 1 at the hearings, said that Bell gave the Polish agents more than 20 highly classified reports on advanced future United States weapons systems. The CIA said the Polish government "probably" gave the reports to the Soviet Union.

The CIA said that among the classified reports Bell turned over to the Polish spies, those of prime importance to the United States included: The F–15 Look-Down/Shoot-Down radar system, the quiet radar system for the B–1 and Stealth bombers, an all-weather radar system for tanks, an experimental radar system for the U.S. Navy, the Phoenix air-to-air missile, a ship-borne surveillance radar, the Patriot surface-to-air missile, a towed-array submarine sonar system, a new air-to-air missile, the improved HAWK surface-to-air missile and a NATO air-defense system. The CIA went on to say:

> The information in these documents put in jeopardy existing weapons and advanced future weapons systems of the United States and its Allies. The acquisition of this information will save the Polish and Soviet governments hundreds of millions of dollars in R & D efforts by permitting them to implement proven designs developed by the United States and by fielding operational counterpart systems in a much shorter time period. Specifications on current and future U.S. weapon systems will enable them to develop defense countermeasures.

Bell, convicted of espionage and serving an 8-year prison sentence, blamed no one but himself for his conduct but he did say that a more effective internal security system at Hughes Aircraft might have pinpointed him as a potential security risk. He said it was well known among his co-workers in the office that his finances were in disarray, that he was being pursued by the IRS and that he had filed for bankruptcy. It also was apparent that he might have harbored deeply felt resentment against the company for which he had worked for 30 years but which, at this late date in his career, had "shunted (me) off to a quiet back room." Bell said his own security clearance with Hughes

had not been reviewed in 28 years. Moreover, Marian Zacharski and his firm, Polamco, were known to the FBI and his association with Bell should have triggered more interest, Bell said.

Bell said FBI agents told him that Marian Zacharski was known by national security authorities to be a "highly trained Polish intelligence officer" when he came to the U.S. in 1977. Zacharski was placed under surveillance "the day he arrived in the United States and when he arrived in California, he was under continuous surveillance there," Bell said.

Convicted of espionage, Zacharski was given a life sentence.

CASE NO. 7 : MARC ANDRE DE GEYTER SOUGHT VALUABLE COMPUTER CODE

Adabas is an acronym for Adaptable Data Base system, a computer program for data base management that is owned by Software AG of North America, a Reston, Virginia firm. According to John N. Maguire, president of Software AG, Adabas includes more than 200,000 detailed instructions and "represents the highest level of sophistication yet achieved" in data base management. The Federal Government estimated Adabas to be worth $10 million. But for Maguire and his firm, Adabas is worth much more. Adabas also is a prize the Soviet Union would like to have.

Testifying before the Permanent Subcommittee on Investigations, Maguire recalled how the Soviets attempted to obtain Adabas. In May of 1979, Marc Andre DeGeyter, a 31-year-old Belgian with financial ties to the Soviet Union, offered $150,000 to Jim Addis, a Software AG executive, for Adabas. DeGeyter said he was making the offer on behalf of the Soviet Union. Addis relayed DeGeyter's proposal to Maguire; Maguire notified the FBI.

Working with the FBI, Maguire negotiated with DeGeyter over the next 7 months. During these discussions, DeGeyter told Maguire that he was in the business of obtaining U.S. technology for the Soviet Union and that the Soviets were anxious to obtain the secret Adabas code.

DeGeyter told Maguire that by selling Adabas to him, he need not fear that the Soviets would divulge its contents to his company's competitors. Maguire recalled:

> DeGeyter assured me that the source code would not be coming back to the States or to American competitors anywhere. He told me . . . the Soviets had no interest in furnishing the code to my competitors.

As time went on, DeGeyter raised his offer, first to $200,000, then to $250,000 and his final proposal was $450,000. However, when Maguire continued to raise objections to certain aspects of the deal, negotiations broke off.

In February of 1980, DeGeyter, feeling that he would not obtain the Adabas code directly from Maguire, asked Charles Matheny, the owner of another Northern Virginia computer firm, if he would help him obtain Adabas. Matheny, whose Centec company was located in the same building as Software AG, notified the FBI.

Matheny arranged to have a Software AG "employee" meet with DeGeyter. The employee was an FBI undercover agent, Timothy B.

Klund, who, on May 18, 1981, encountered DeGeyter at the John F. Kennedy International Airport in New York. DeGeyter gave Klund a check for $500,000. Klund gave DeGeyter a computer Software tape, purportedly the Adabas system. FBI agents arrested DeGeyter. The tape was a fake. The DeGeyter bank account was found to contain only $800.

Software AG president Maguire told the subcommittee that when DeGeyter was arrested he assumed, "perhaps naively," that the Soviets' efforts to buy Adabas had ended. But he soon realized that the Soviets still wanted Adabas and "are, in fact, still trying to secure it."

Maguire said Georgiy V. Veremey, a Russian diplomat in the United States, visited the Software AG booth in two trade shows in Washington, D.C. in 1981. On both occasions, Veremey asked numerous questions of Software AG spokesmen about Adabas materials and its source code.

After the trade show contacts, Veremey visited Software AG offices in Reston on September 25, 1981. He introduced himself as being a member of the Soviet Embassy staff in Washington and asked for publications about Software AG products, Maguire said.

In a discussion with Sunday Lewis, a Software AG executive, Veremey asked for a complete bibliography of all the firm's products. Veremey disclaimed any particular purpose for the request, saying he was just "interested." Maguire said Veremey was vague about the kind of work he did at the embassy. Lewis gave him a standard list of publications and an order form and he left. Lewis reported the incident to Maguire.

On October 2, 1981, Georgiy Veremey returned to Software AG. While waiting for Sunday Lewis to return from lunch, Veremey "continually wandered in and out of Software offices," Maguire said. The receptionist asked him to remain seated but he would not. When Lewis arrived, Veremey told her he wanted to order all Software AG's documents. Maguire testified as to what he felt was the significance of Veremey's request:

> At a price of about $400, the documents would fill about 12 boxes. This type of technical documentation tells one how to use various systems produced by Software AG. One would have no use for this unless (1) you have the system or are planning on acquiring it; or (2) you are planning to develop the system via knowledge of user techniques.

Maguire said Lewis told Veremey that she could not sell him the documentation, that to do so would require approval from the Federal Government. Maguire said Veremey laughed and replied, "What license was issued for the U.S.-U.S.S.R. wheat deal?" Maguire said Veremey left Software AG and had not returned.

Maguire said subsequent requests to obtain Adabas have come to Software and its distributors from the Hungarian Embassy in Washington, D.C., Germany and Japan as well as Polish sources.

Maguire was critical of the Federal Government for the mild punishment given Marc DeGeyter. Indicted on charges that he was guilty of interstate and foreign travel in aid of a racketeering enterprise (18 U.S.C. 1952(a)(3)), DeGeyter was permitted to plead guilty to misdemeanor violations of the Export Administration Act and the Vir-

ginia Commercial Bribery Statute, adopted as a Federal offense under 18 U.S.C., section 13. He served a sentence of 4 months, was fined $500 and paid a $10,000 civil penalty to the U.S. Department of Commerce.

Maguire contrasted DeGeyter's 4-month prison term with the 7 months of his own time he had given up to work with the FBI in building a possible case against DeGeyter. Maguire testified:

> In the DeGeyter case, I spent nearly 7 months dealing with a man openly working for the Soviets to purchase one of the most significant trade secrets in the U.S. software industry. Despite that fact, he was eventually charged only with misdemeanors under commercial bribery statutes. In my mind, it is entirely incomprehensible that the man was finally sentenced to a jail term of merely 4 months.
>
> By comparison, I read newspaper reports of a Celanese corporation employee who in June, 1979 was convicted and sentenced to a term of 40 years for selling trade secrets to Mitsubishi Plastics Company, a Japanese competitor of Celanese. From the scant newspaper reports, I can glean no evidence of national security interests or Soviet involvement. In sum, a businessman received 40 years for selling trade secrets to a competitor while a Soviet agent receives 4 months for attempting to transfer one of our most guarded technology secrets to the U.S.S.R. It is, indeed, a sad state of affairs if those cases accurately reflect this country's priorities on technology transfer.

Theodore S. Greenberg, an Assistant U.S. Attorney in the Eastern District of Virginia, prosecuted DeGeyter. In his appearance before the Investigations Subcommittee, Greenberg was asked why the charges against DeGeyter were dropped from felonies to misdemeanors. "There were significant governmental considerations which I would be happy to disclose to the subcommittee in closed session," Greenberg testified.

Greenberg said that when DeGeyter completed his 4-month prison sentence, he was released to an Immigration and Naturalization Service detainer stemming from the fact that during his imprisonment his visa had expired. Greenberg recommended to INS that DeGeyter be deported immediately. INS replied that because DeGeyter had been convicted of a misdemeanor not involving moral turpitude he "was not required to depart the country involuntarily," Greenberg said, adding that it is his understanding that DeGeyter is free to reenter the U.S.

CASE NO. 8: WALTER SPAWR SOLD LASER MIRRORS TO THE SOVIET UNION

Theodore Greenberg, testifying about the DeGeyter case, was one of two Assistant U.S. Attorneys with experience in technology diversion prosecutions who gave the subcommittee information on their experiences in bringing such cases to trial. The other prosecutor was Theodore W. Wu, an Assistant U.S. Attorney in Los Angeles. Being a graduate in engineering from the Naval Academy in Annapolis, a former Naval officer and an officer in the Naval Reserve, Wu was unique among Federal prosecutors because of his military and technical background and expertise.

Wu, whose prepared testimony was submitted into the hearing record, handled the prosecution in two major diversion cases—the CTC-Maluta case, which was described earlier in this report; and the Spawr case.

Wu said that in 1974 and 1975, Walter Spawr, president of Spawr Optical of Corona, California, sought new markets for the laser mirrors his firm produced. He turned to Europe. In West Germany, he hired Wolfgang Weber, a young and ambitious salesman with contacts in the Soviet Union.

Weber exhibited Spawr mirrors in Moscow late in 1975. Mashpriborintorg, the Soviet purchasing agency, placed an order for Spawr Optical water-cooled mirrors through Weber. Describing the mirrors, Wu said:

> These mirrors of various diameters ranging up to 12 inches were the finest manufactured by Spawr Optical, which was noted in its field for the superior quality of its mirror surfaces.

Spawr, enthusiastic about filling the order from Mashpriborintorg, knew that Federal law required that before exporting the laser mirrors to the Soviet Union he had to obtain a validated export license from the Commerce Department. Not to do so would constitute violation of the Export Administration Act. Wu said Spawr did not apply for such a license and exported the mirrors anyway.

Spawr shipped most of the laser mirrors to the Soviets in July of 1976. Wu said export documents containing false statements were filed by Spawr and his wife Frances "to evade scrutiny and export licensing requirements."

Not only did Spawr know that what he was doing was illegal, he also knew of the military consequences of his action. He was no newcomer to the national security field. Wu said Spawr Optical held a Defense Department facility security clearance and had performed contracts on government defense programs. Spawr Optical had performed laser optics polishing work for TRW and Rocketdyne and the Los Alamos National Laboratory, the Redstone Arsenal and the Naval Weapons Laboratory. Spawr Optical had furnished the Air Force Weapons Laboratory at Kirtland Air Force Base, New Mexico with high energy laser mirrors "of the identical specifications as some of the mirrors illegally sold to the Soviet Union," Wu said.

Mashpriborintorg ordered more water-cooled mirrors. This time the Spawrs applied for an export license. The Commerce Department, citing national security reasons, rejected the request.

When the Commerce Department rejection letter arrived, Spawr tried to conceal the true destination of the planned shipment by having Wolfgang Weber wire a bogus cancellation of the order. Spawr Optical employees were told to quit talking about their large "Russian" order.

Using false Shipper's Export Declarations, Spawr Optical began shipping the second order of mirrors to the Soviet Union through Switzerland in February of 1977.

The illegal shipments, first detected and investigated by the Compliance Division of the Commerce Department in February of 1978, resulted in a Federal grand jury returning indictments against Spawr

Optical and Walter and Frances Spawr. The Spawrs and their firm were convicted on December 12, 1980 of conspiracy, submission of false statements and illegal exportation of laser mirrors to the Soviet Union. Frances Spawr was sentenced to 5 years' imprisonment, but her sentence was suspended and she was placed on probation for 5 years. Walter Spawr received a sentence of 10 years, all but 6 months of which was suspended. He received 5 years probation. Both Spawrs were ordered to contribute 500 hours to a charitable organization. Their company was fined $100,000.

Wu quoted Colonel Bob L. Francis, Commander of the Air Force Weapons Laboratory, who said the mirrors exported by Spawr Optical not only advanced the laser mirror technology in the U.S.S.R., an area where the Russians were felt to be deficient, but also saved the Soviets millions of dollars and nearly 100 man-years in research and development. Francis said that even though the commercial value of the mirrors was relatively low, at about $60,000, the technological value received by the Soviet Union was much more.

A VIEW FROM INSIDE THE SILICON VALLEY

The subcommittee received a comprehensive and detailed description of the difficulties faced by law enforcement in trying to control the export of high technology from a local prosecutor, Douglas K. Southard, Deputy District Attorney in Santa Clara County, site of "Silicon Valley," a massive concentration of this Nation's integrated circuit manufacturing industry.

Southard, who, as a lawyer, had no technical background before being assigned high technology fraud, theft and trade secret prosecutions 3 years ago, taught himself the basics of integrated circuitry and gave the subcommittee simple explanations of the fundamental concepts involved. Dr. Lara H Baker, Jr., of the Los Alamos National Laboratory, a renowned computer scientist who also testified before the subcommittee, was shown a copy of Southard's testimony. Dr. Baker had enthusiastic praise for Southard's grasp of the subject.

Southard testified that the integrated circuit or IC was invented in the late 1950s. Suggesting that integrated circuitry may be the most significant technological breakthrough since the industrial revolution, Southard said that when, in 1971, in Santa Clara County, an entire computer was produced on a single chip, the first step had been taken in revolutionizing the electronics industry. Southard added:

> Continued development of integrated circuit memory chips has reduced the cost of information storage in computers a hundred fold in the last 10 years. In the late 20th and early 21st centuries, integrated circuitry will be as basic to an industrial economy as steel in the 19th and early 20th centuries. Leadership in this technology will be vital to any nation that would be a world leader in economic and military power.

Silicon Valley[6] firms pioneered the development of integrated circuitry. The area is today among the world's most competitive in IC

[6] The Silicon Valley got its name from the fact that the non-metallic element Silicon (Si) is an essential ingredient in integrated circuits. The "valley" is in the general vicinity of Stanford University and includes communities such as Palo Alto, Mountain View, Los Altos and Sunnyvale.

technology and manufacture. Its products can be found in all types of commodities, from microwave ovens to video games to the most sophisticated military weaponry. Growth has been rapid, but expansion has not been accompanied by concern for security. As a result, Southard said, there has been a "substantial lag in public and official appreciation of the national security implications of the new technology." The industry has neglected to police itself. Southard quoted a senior executive of one of the largest integrated circuit companies as having remarked recently, "Hey, we're in the chip-making business. That's the Fed's problem to worry about where it goes afterwards." Callous as the remark was, it was somewhat representative of the industry, Southard said.

Southard said that in the last 5 years there had been about $100 million in thefts of electronic technology and commodities in Santa Clara County. He warned:

> We in law enforcement have only recently, within the last 3 years, almost stumbled across the problem. At the time, we were totally unprepared to deal with it. Now we are beginning to make some headway.

Most of the thefts in the integrated circuit industry are the work of employees—technicians, inventory clerks, draftsmen, engineers, even security personnel, Southard said. Many of the valuable components and systems of high technology electronics are so small that thievery is tempting and easy to get away with. Valuable production tools incorporating all details of a sophisticated new circuit design, for example, can be taken out of a plant in an employee's coat pocket.

Southard said countries such as those in the Soviet Bloc which do not have the technical expertise to design their own integrated circuity components and systems will try to obtain such equipment illegally. In this way, the less developed nations can develop the ability to manufacture certain integrated circuitry without being required to design it.

The most common form of theft in the Silicon Valley, Southard said, occurs when an employee steals large numbers of chips—as many as a thousand—by filling his briefcase or the lining of his jacket. The thief, often a middle class professional leading an ostensibly respectable life, can sell the chips below market value to brokers, who rarely insist on knowing where the items came from.

Typical of this kind of theft, Southard said, was a recent one involving the president of a parts distribution firm. The man was successful, had a hillside home, a beautiful wife, children in private schools and a Mercedes. He was discovered selling stolen integrated circuits to Werner J. Bruchhausen, a West German, Southard described as an "internationally known fence" who "is widely reputed to be a Soviet East German agent."

The reason for the executive's conduct, Southard said, was greed, but a special kind of greed perhaps unique to the Silicon Valley:

> This kind of greed is not unusual in the context within which he worked: Silicon Valley, a prime example of capitalism on the rampage. Everyone wants to become an overnight millionaire and money flows like water, tempting the otherwise honest citizen to scramble fast to get his share of the pie.

Southard cited three investigations—the Lowery, Jackson and Gopal cases—which, he said, are informative as to the problems law enforcement faces in the Silicon Valley.

CASE NO. 9: $3.4 MILLION THEFT AT MONOLITHIC MEMORIES

Larry E. Lowery, who operated a company known as L & M Electronics in Mountain View, was believed to be involved in the fencing of $100,000 worth of stolen late model integrated circuits. Initially police could not get his accomplices to testify against him and he escaped prosecution.

A second inquiry led police to arrest Lowery when they found his new firm, Brut Electronics, housing 11,000 stolen integrated circuits worth between $100,000 and $150,000. As the county prepared for trial, one prosecution witness was beaten savagely by a stranger and was unable to testify. Another prosecution witness was murdered execution-style and his body dumped in a shallow grave in the Santa Cruz Mountains. Lowery was convicted after a highly technical 6-week trial and was sentenced to 2 years in prison.

While Lowery was free on bail pending appeal, Monolithic Memories, Inc., of Sunnyvale, lost $3.4 million in a Thanksgiving weekend IC theft. A ton of equipment, much of it with military applications, was towed away in trucks, an exercise which police believed was an inside job.

A 3-month undercover investigation—and a talkative fledgling cocaine dealer who worked at Monolithic and claimed to be starting up his drug trade through earnings from the theft—led agents to conclude that Larry Lowery and an associate had masterminded the Monolithic burglary. But, Southard said, proving the allegation will be difficult. He explained:

> To date, the trail of investigation is littered with dead bodies, assault, sophisticated thefts, drug sales and more. Scores of criminal conspirators appear to be involved. It represents the clearest case of consistent, habitual, organized criminal activity aimed at Silicon Valley as yet uncovered. Because of the complexity of the case and the circumstantial nature of the evidence available, it would be a very difficult task to fully prosecute all the people involved. Undoubtedly, it will take years before the investigation is completed and prosecutions culminated.

CASE NO. 10: STOLEN INTEL EQUIPMENT FOUND IN MUNICH

The second case cited by Southard involved John Henry Jackson, a felon convicted five times for theft and forgery but who had never been sent to prison for these crimes. An anonymous caller and a subsequent undercover investigation resulted in a court-authorized search of Jackson's residence where thousands of stolen integrated circuits were seized.

Further inquiry tied Jackson to the theft of about $1 million in integrated circuits from the Intel Corporation, and to stolen, counterfeit and substandard integrated circuits that were traced to firms in Arlington, Virginia; Torrance, California; and Munich, West Germany.

The Jackson case is still pending trial, Southard said, admitting that the prosecution is of such a complex, technical nature that he foresees problems ahead in finding direct evidence that will establish knowing receipt of integrated circuits. Stolen chips look just like honestly obtained chips and proving which are stolen and which are not when they have been combined can be an impossible job. Few brokers in the integrated circuit business maintain records sufficiently specific to establish an audit trail. "Nor are knowing thieves likely to keep such records," Southard said, adding:

> Finally, the cost for such a prosecution would be almost prohibitive for a local jurisdiction. The estimated cost of producing the minimum one dozen witnesses from Europe and the East Coast necessary to prove the evidentiary chain in the Jackson case is in excess of the entire witness budget for the County of Santa Clara for an entire year. Public safety considerations simply will not allow property crime prosecutions to take precedence over violent crime prosecutions.

CASE NO. 11: SILICON VALLEY FIRM OWNED BY ALLEGED BLOC SPY

Southard's third case had strong national security implications. Yet the case was handled by Santa Clara County law enforcement officials.

The case revolved around Peter K. Gopal, part owner of a Silicon Valley electronics firm. Gopal came to the attention of authorities in early 1978 when Intel Corporation learned from an anonymous source that a competitor, National Semiconductor Corporation, was in possession of a computer data base tape containing the design of a late model Intel microprocessor chip.

A suspect said Peter Gopal had been involved. Further inquiry, including undercover investigation, developed more information implicating Gopal. In one taped conversation, Gopal offered to sell original Intel chip design information for a price of millions of dollars; and said he had already sold certain designs in Europe and that his foreign clients were very satisfied with his product.

Later Gopal sold Intel chip designs to undercover agents. Millions of dollars of additional integrated circuit designs and related products were found in court-authorized searches of Gopal's business. Also seized were records indicating that Gopal had met with officers of the Soviet Consulate in San Francisco and had made numerous trips to Europe, Poland and the Soviet Union in 1977 and 1978. It was also established that Gopal's partner was Dr. Rudolf Sacher of Vienna, believed by law enforcement and intelligence authorities to be part of an East Germany spy network.

When the Commerce Department found insufficient evidence to prove a Federal violation more serious than a misdemeanor, Southard prosecuted Gopal on various State felony laws, including conspiracy, bribery, to obtain trade secrets and theft and possession of stolen trade secrets.

The court would not allow evidence seized in the searches because of what Southard termed a "novel problem." Police conducting the searches were not trained in electronic high technology and were not sure of what items to search for. So they brought with them technical

experts not affiliated with law enforcement. The judge ruled that the police had abdicated their responsibility of personally conducting the search by bringing along outsiders. On appeal, the seized evidence was reinstated.

Gopal was convicted of six counts of receiving and possessing stolen trade secrets, bribery and conspiracy. He was sentenced to 2 years and 8 months, but is currently free on bail pending appeal, which is expected to take at least a year. Southard said:

> The transcript of the proceedings has not yet been transcribed, it was so voluminous. Three and one-half years after the offense and one year after conviction, Mr. Gopal has yet to go to jail.

Southard said cases of this magnitude tax the resources of Santa Clara County and assistance from the FBI would have been of benefit, particularly in light of the Rudolf Sacher connection and other national security considerations.

Southard said the Gopal case represented one of the first major prosecutions under California's Trade Secret Theft Statute. He went on to say:

> The statute . . . is a departure from traditional common law notions of property subject to theft. At common law, property must be physical to be subject to theft. The Trade Secrets law expands this concept of property by specifically making ideas qualify as Trade Secrets property for purposes of penal statutes. This statute was designed to fill some of the logical gaps in the law by existing patent and copyright legislation. It protects ideas which are not patentable nor copyrightable, but which have substantial business value to its owner or competitors. For instance, a semiconductor device, such as a "memory" device would not be patentable because it is not a product of new technology, but merely builds upon existing technology. Under copyright law it would not be copyrightable even though such a design is in large part based upon its designer's creativity. Yet such a design can and increasingly does represent the expenditure by its owner of hundreds of thousands, even millions, of dollars of manpower, time and materials, before a single chip can ever be produced.

A VIEW FROM INSIDE THE SOVIET UNION

In the Gopal case, Santa Clara County prosecutor Douglas Southard showed the subcommittee one route through which the valuable integrated circuit technology can make its way to the Soviet Bloc. But U.S. authorities could not say from firsthand experience how the Soviets utilize such products. For information on that question, the subcommittee turned to a former Soviet engineer who had worked in reverse engineering and other technology transfer programs managed by the Kremlin.

Using an assumed name and testifying behind a screen to protect his family's and his identity, "Joseph Arkov," an emigre who came to the U.S. in 1979, told the subcommittee that the Soviet government wants to develop its own ability to produce high technology equipment simi-

lar to that manufactured in the West and Japan. To achieve that goal, the Soviet technical institutes allocate a certain amount of money to be used for the purchase of Western, particularly American, technology.

Arkov said the Soviet Union has two goals when it seeks to obtain Western technology. One objective is to study the equipment with the intention of imitating or duplicating it. The second objective is to use it in the manufacture of other high technology components. "The second goal—the use of the machinery—is, by far, the most important to the Soviets," Arkov said. He explained:

> The Soviet government benefits to a certain extent from its programs aimed at duplicating Western technology, but the results have been, and will continue to be, limited. Soviet authorities have come to the realistic conclusion that their country's level of technology is too far behind the West for them to make great strides through copying. They do not have the human resources or the fine tuned equipment required to copy. Once they know what makes a given piece of machinery work, they find that they do not have the technical know-how and equipment to produce the product themselves. That is why they want Western high technology machines that will enable them to produce the products. And the Western products they desire the most are those produced in the United States. . . .
>
> By using—not copying—the American high technology products, they move closer to their goal of technical self-sufficiency. Whether they will ever become self-sufficient in high technology is a debatable point. My own view is that this course of action gives them quick gains, but, over the long run, it will result in their being permanently behind the United States, forever having to rely on American products to manufacture their own.
>
> However, being behind us in technology is a relative condition. The Soviets can make progress in a technical sense and, at the same time, trail the United States but, by their standards, they will have achieved much. Their accomplishments will have been made with limited cost to them because the basic research and development will have been paid for by the Americans.

Arkov stressed the importance of the Soviets' decision to use—and to rely less on copying—U.S. technology. He recommended that American export policy take this distinction into account.

Pointing out that there are very limited applications for high technology items such as integrated circuits and lasers in the Soviet civilian economy, Arkov said Russian planners assign all such commodities to enhancing their nation's military prowess. He went on to say:

> In most fields of technical research, development and production which I am familiar with in the Soviet Union. the overwhelming majority of resources are invested in military applications. If, in the area of high technology obtained from the United States one much prized oscilloscope is obtained

> from the U.S., it will be turned over for military application in virtually every instance. This strengthens the position of the U.S.S.R. armed services but it is done at the expense of the civilian sector. The oscilloscope might have been used in the development of a consumer product but rarely are such high technology devices ever utilized to benefit the Soviet citizen as a consumer. As a matter of fact, the Soviet industrial capacity is so completely overburdened with military production that the Soviets could not make a civilian or commercial application of certain high technology products even if they wanted to. For example, there is almost no possible way the Soviets could make a civilian application of laser technology. Any laser component they obtain from the U.S. will go into the military sector. The Soviets have no other use for it. There is no commercial market for high technology equipment in the U.S.S.R. People cannot afford such luxuries yet the government displays it for propaganda purposes. Most equipment is used by the Soviet military industry.

Arkov said the Soviets promptly translate into Russian technical journals and government documents from the U.S. and distribute them to their scientists and engineers. He said trade fairs are a frequent target of Soviets trying to obtain Western technical data. He said student exchanges with the U.S. are seen by the Soviets as opportunities to obtain American technology while revealing little of what is happening technically in the U.S.S.R. Recalling his own college days, Arkov said ordinary students were never selected for exchange programs. Only established scientists and engineers were chosen, he said, adding:

> The Soviets considered college age students to be too young and unpredictable to be trusted to attend universities in the United States. Equally important, we—ordinary students—had not yet advanced far enough in our studies and knowledge to obtain the high level of information Soviet authorities desired.
>
> Soviet authorities selected participants in the student exchange programs from science and engineering. Conversely, American exchange students might be from the humanities; they might come to the Soviet Union to study Dostoyevski. But the Soviet students did not go to the United States to study Faulkner. Their purpose in the U.S. was to obtain American technology. In the engineering classes I took in college, I met students from Cuba, North Vietnam and Hungary but no Americans.

Arkov and his family live in Los Angeles County where he is employed as an engineer.

INTENTIONAL
BLANK

IV. Staff Recommendations on Commerce and National Security Agencies

Remedies Proposed in Both Aspects of Preliminary Staff Inquiry

At the hearings, the minority staff of the subcommittee presented its evaluation of the effectiveness of the executive branch in enforcing export controls. After a preliminary investigation of more than a year, the minority staff submitted its findings to the subcommittee in two categories. First was an evaluation of the Commerce Department in enforcing the Export Administration Act, the principal statute concerning the sale abroad of non-classified technology. The second aspect of the staff's preliminary inquiry had to do with the extent and participation of defense and intelligence agencies in export control efforts. In both instances, the staff said improvements needed to be made and proposed recommendations for corrective action.

Commerce Department Enforces Export Administration Act

The subcommittee investigation focused major attention on "dual-use" technology; that is, technology developed or manufactured in the United States by the private sector mainly for commercial purposes but which in the hands of the Soviets or another adversary can have military applications threatening U.S. national security.

Militarily critical dual-use technology cannot be exported legally without a validated export license from the U.S. Department of Commerce. Procedures for the export of such technology are spelled out in the Export Administration Act of 1979.

Since the end of World War II, the U.S. has maintained controls on exports for the purpose of pursuing national security, foreign policy or domestic economic objectives. According to the Library of Congress,[6] export controls have been used most frequently for national security purposes, primarily to restrict U.S. exports to the Soviet Union and other Communist countries.

The first major postwar control legislation—the Export Control Act of 1949—established controls on all exports to Communist countries. Controls were relaxed gradually in the late 1950s and throughout the 1960s.

The Export Control Act was amended and extended several times through 1969, when it was superseded by the Export Administration Act of 1969. The new act maintained export controls but called for a removal of constraints on goods and technology readily available to Communist countries from non-U.S. sources and on items of marginal military value. The Library of Congress study described the significance of the Export Administration Act of 1969 this way:

[6] "Foreign Espionage and U.S. Technology," a report prepared at the request of the Senate Permanent Subcommittee on Investigations by the Congressional Research Service of the Library of Congress, April 12, 1980; and received as Exhibit No. 22 at the subcommittee hearings.

The 1969 legislation represented a new mandate for export controls. Whereas the thrust of the Export Control Act of 1949 had been to limit East-West trade, the 1969 act was designed to foster such trade.

The 1969 act was amended in 1972, 1974, and 1977 and was replaced by the Export Administration Act of 1979. The 1979 law maintains the basic emphasis on export expansion that was introduced by the 1969 act. The law will expire on September 20, 1983.

Under the Export Administration Act, the U.S. Department of Commerce, through its Office of Export Administration has jurisdiction over most non-classified exports from the United States territories and possessions. Goods or technical data exported to any country except Canada are required to be licensed.

Most U.S. exports are made under a general license, which is a general authorization to ship certain types of goods and technology to specified destinations without a specific application by the exporter. Goods and technical data of a more sensitive nature which may not be exported freely require a validated license, which identifies the type, quantity and destination of the export.

The Export Administration Act provides penalties, including fines, denial of export privileges and imprisonment, for violations.

RECOMMENDATION WAS MADE TO PLACE ENFORCEMENT IN CUSTOMS SERVICE

The Commerce Department enforces export controls through its Compliance Division located in the Department's Office of Export Administration. The staff's evaluation of the Compliance Division was based on provisions of the Export Administration Act that mandated that enforcement be carried out in light of national security considerations. The evaluation also was made with reference to the Division's capabilities as a law enforcement organization.

The staff concluded that the Compliance Divison was an understaffed and poorly equipped and, in certain instances, undertrained and unqualified investigative and intelligence unit. Its investigators numbered eight to eleven agents; its inspectors totaled five or six; and its intelligence section had three to five analysts. There were no requirements relating to the training and experience of personnel. Some agents were well trained because of previous work. Other agents were not formally trained. Agents were not authorized to make arrests, search and seize questionable exports, or carry firearms. Paradoxically, they did undertake traditional law enforcement exercises such as surveillances of suspected violators. In these exercises, operations were directed by inadequately trained supervisors.

One Compliance Division agent, an investigator, who, unlike several of his colleagues, did have extensive law enforcement experience and training, told the subcommittee staff the unit was "totally ineffective" in preventing dual-use technology from being shipped to the Soviet Bloc. He said the Kremlin's spy organization, the KGB, could not have organized the Compliance Division in a way more beneficial to Soviet interests. "This agent's view was not contradicted by persons in the law enforcement and national security field," said subcommittee investigator Fred Asselin, who presented the staff's evaluation of the Compliance Division.

However, the same law enforcement and national security officials who would point to shortcomings in the Compliance Division refused to come forward and acknowledge such deficiencies before the subcommittee. The staff asked the FBI, the Nation's preeminent law enforcement organization, to provide assistance in evaluating the Compliance Division. The FBI refused. A similar request was made of the Justice Department and the U.S. Customs Service. Again, officials refused. Asselin testified that it had been the staff's hope that other law enforcement organizations would come forward and critique the Division in a constructive and professional manner. "In this pursuit," he said, "we were met with resistance. Working agents and senior officials alike would be candid, while insisting on their anonymity." Asselin went on to say:

> . . . the result of this reluctance to criticize constructively the Compliance Division in public session leads to the current situation in which the only evaluation the Congress hears is from the Commerce Department, which houses the Division and which is less likely to make a candid and forthright evaluation of the shortcomings of one of its own components. For that reason, it seemed important to the minority staff that Congress be informed about the widespread dissatisfaction that exists in the executive branch concerning the Compliance Division and the principal reasons for that dissatisfaction.

The staff's principal recommendation was that the Compliance Division be abolished and its duties taken over by the Customs Service. The staff presented these additional findings:

1. The Commerce Department had overstated the effectiveness of the Compliance Division in reports and testimony to Congress.

2. The Commerce Department has as its major focus the promotion of trade and is not comfortable with the task of limiting the sale of anything, whether it is dual-use technology or some other commodity. In this finding, the staff cited a similar conclusion reached by Senator Jake Garn of Utah, who, in introducing legislation to create an Office of Strategic Trade, has referred to the "export promotion bias" of the Department as making it unfit to enforce export controls.

3. The Commerce Department has limited tradition and expertise in traditional law enforcement. Even though the Department has had the responsibility to investigate export control violations for 30 years, its senior officials had not seen to it that basic law enforcement procedures were followed—in hiring practices, in the training of agents, in the conduct of investigations and in other matters.

4. The Compliance Division had a large backlog of cases, with 200 to 400 in the Investigations Branch and 600 in the Intelligence Branch. So many cases hovering over the small investigative staff could create pressure on agents to close cases without adequate inquiry. The large backlog in Intelligence can cause delays throughout the system because many cases begin there.

5. Demonstrative of the Compliance Division's shortage of trained personnel was the fact that in 1980 when the Division was given the assignment of investigating violations of the grain embargo against the Soviet Union, only one agent was used to carry out that mission.

When other components of government learned of the limited resources the Compliance Division had for this responsibility, the Department of Agriculture, the Central Intelligence Agency, the State Department, the Navy and other agencies formed an inter-agency working group to monitor grain exports and provide for an exchange of information with the Commerce Department. However, the principal investigative function—that is, the responsibility to look into allegations of violations of the embargo--remained with the Commerce Department. The duty rested with one agent, a GS–12 in the Compliance Division. On the grain embargo issue, subcommittee investigator Asselin testified:

> The minority staff inquiry found that the inadequate response of the Compliance Division in enforcing the grain embargo demonstrates the serious government operations problem in which the most senior officers of the executive branch, from the President on down, shape policy and promulgate directives on the mistaken premise that the affected agencies have the necessary means to turn the policy and directives into reality. President Carter's grain embargo speech might have been received in a different light had he also announced that the Commerce Department would assign one man—a GS–12 in the Compliance Division—to investigate alleged violations.

6. There was a lack of harmony between the Compliance Division and the Customs Service. The result was that effective enforcement was reduced. Part of the tension stemmed from the Commerce Department's strict interpretation of the proprietary information provision in the Export Administration Act. Customs agents complained that they were being denied information they needed to carry out investigations of export violations. Tension also was caused by Customs' sense that the Compliance Division's inexperienced personnel were involving themselves improperly in Customs' foreign work, risking the compromise of on-going cases, causing confusion and uncertainty among foreign officials and having a negative impact on the national security.

7. The staff submitted a detailed narrative of the government's investigation of the CTC-Maluta syndicate, a network of companies in Southern California and Western Europe whose illicit exporting activities resulted in the transfer from the United States to the Soviet Union of more than $10 million in dual-use high technology, much of it for the building and equipping of a Soviet plant for the manufacture of semiconductors. Believed by many law enforcement experts to be one of the most important technology diversion cases ever mounted, the CTC-Maluta investigation demonstrated the many shortcomings in the Compliance Division and provided sufficient evidence to support the staff's principal conclusion that enforcement of export controls should reside in the Customs Service.

Inexperienced in major investigations, unable to devote the necessary trained personnel to traditional law enforcement undertakings, equipped with none of the tools traditional law enforcement agencies use routinely, the Compliance Division was an unnecessary participant in the CTC-Maluta case, according to the staff's findings. The CTC-

Maluta inquiry revealed that there is nothing the Compliance Division can do that cannot be done more efficiently and more professionally by a traditional law enforcement organization such as the Customs Service. In his testimony, subcommittee investigator Fred Asselin noted that the Commerce Department, in its 1981 report to Congress, sought to take credit for the CTC-Maluta case. This was inappropriate, he said, explaining:

> In fact, the CTC case does not qualify as a Commerce Department investigation. Customs Service agents did most of the work; and executive supervision was provided by Assistant U.S. Attorney Theodore Wu and Kenneth Ingleby, Chief of the Customs Service Investigations Office in San Pedro. . . .
>
> After the CTC case was brought to Wu, the Compliance Division played no essential role in the inquiry. That recognition leads to the minority staff's finding, which is that the Commerce Department should not have the enforcement function under the Export AdministrationAct.
>
> It is the finding of the minority staff that the national security implications of enforcement of the Export Administration Act are too important to be entrusted any longer to the Commerce Department as presently organized.
>
> For three decades the enforcement function has resided in the Commerce Department—through administrations controlled by Democrats and Republicans. Three decades is sufficient time to allow reasonably capable officials to perfect the most challenging task. But serious procedural and operational problems still exist in the Compliance Division of Commerce. We find the conclusion inescapable, therefore, that effective enforcement of the Export Administration Act is beyond the institutional capabilities of the Commerce Department.
>
> Moreover, from a government operations and executive organizational standpoint, the mere existence of the Compliance Division is an impediment to efficient and effective enforcement of the act. Understaffed, flagrantly short of resources, the Division cannot do the job effectively; but, by its presence, prevents other components of government from taking on the task.

The staff offered two solutions for the subcommittee's consideration—one short term, one long range. Immediate relief could be found if the Compliance Division were abolished and all its functions placed in the Customs Service.

> This action would insure that competent, professional agents, trained in formal, traditional law enforcement procedures, would be assigned to investigate alleged violations of the Export Administration Act; that they would work under the supervision of executives who also would have formal, traditional law enforcement backgrounds; and perhaps most important of all, the entire function would exist in a Cabinet-level Department with longtime experience in and commitment to traditional law enforcement.

In terms of longer range considerations, the staff recommended that the subcommittee consider the proposal put forward by Senator Garn to create an independent Office of Strategic Trade that would absorb the Commerce Department's Office of Export Administration.

LAWRENCE BRADY DISAGREES WITH STAFF RECOMMENDATION

Lawrence J. Brady, Assistant Secretary for Trade Administration in the Commerce Department, was responsible for the activities of the Compliance Division. Brady, who, before joining the administration as a Presidential appointee in 1981, had been one of the most severe critics of the Commerce Department's export policies and practices, testified before the subcommittee.

The subcommittee staff's principal recommendation—that of abolishing the Compliance Division and placing the enforcement function of the Export Administration Act in the Customs Service—was wrong and he would oppose it, Brady said, pointing out that Customs agents did not have sufficient technical expertise to be the "lead" enforcement arm under the statute. Characterizing the subcommittee staff's evaluation of the Compliance Division as a "useful historical document," Brady did not contest any single point in the staff's indictment of the Division, except to say that it was dated and had relevance only to past administrations. Of the staff critique in general, Brady said:

> . . . it does not recognize that the policies of this administration represent a sharp change from the practices of the past; that we view the pressing need for more effective (export) control as a top priority.

Brady, who, in testimony before the investigations subcommittee in 1980, said the Commerce Department allowed its preoccupation with trade promotion to undermine national security considerations, testified that the Department now had a new way of doing things, that it was now very sensitive to Soviet technology acquisition efforts and was capable of blunting them. He did not say, however, specifically how the Compliance Division had been improved.

In response to questions from Senator Nunn, Brady acknowledged that the changes he said he had made were largely ones of intent and resolve and that as of the day of the staff presentation—May 5, 1982—the Compliance Division was operating with resources and authorities very much similar to those it had had during the previous administration. Brady said there were substantial organizational improvements being planned that would enlarge the numerical strength of the Compliance Division, upgrade its professional standards as a law enforcement entity, make it more efficient and give the enforcement function itself more influence in Departmental decisionmaking. But none of these planned improvements had been implemented.

Senator Nunn said that the Inspector General's Office of the Department of Commerce had conducted a 5-week inspection of the Compliance Division. The inspection had been completed as recently as the day before. Senator Nunn said the IG's findings with respect to the effectiveness and efficiency of the Compliance Division were similar to, and supportive of, the conclusions reached by the subcommittee staff.

Addressing Brady, Senator Nunn said:

I want to make it clear to you and everyone that the problems we are outlining about the Commerce Department and the Compliance Division are directed at not just this administration, but the previous administration and the administration before that. This is a longstanding problem and has no partisan origin and no partisan conclusion. It certainly does not relate to you because a good many things we are talking about have been ongoing problems.

IMPROVEMENTS SAID TO BE NEEDED IN ROLE OF DEFENSE AND INTELLIGENCE AGENCIES

In its preliminary investigation into export controls, the minority staff of the subcommittee examined the efficiency and effectiveness of the executive branch in obtaining and utilizing intelligence information concerning the Soviet Union's programs to acquire Western technology. Also examined was coordination among the Departments of State, Defense, Justice and Commerce, the U.S. Customs Service and other agencies as they shaped and executed export control policy.

Presenting the minority staff's preliminary findings, subcommittee investigator Glenn Fry testified that the principal conclusion of the investigation was that the national security agencies of government had not made technology transfer a sufficiently high priority. This was corroborated by Admiral Bobby R. Inman, Deputy Director of the CIA, who testified that, "The whole question of technology transfer has not been a priority topic."

Fry testified that even if the Commerce Department had enforced the Export Administration Act in a more effective manner it would still not have been enough to halt or delay the flow of technology to the Soviet Bloc. Enforcement, he said, was a critical aspect of export controls, but not the only aspect. Defense and intelligence agencies must contribute as well. He said:

> Ineffective control of the transfer of U.S. technology and the enforcement of export laws will prevail if the Department of Defense and the intelligence community continue to provide less than their best efforts to support this national security mission. Despite several previous congressional investigations and hearings conducted on these matters, dating back to 1974, the responsible executive branch agencies continue to have difficulty in organizing an effective operation.
>
> Technology transfer can occur through the illegal export of controlled or embargoed commodities; however, it can also occur, with equal damage, because of inadequate control and protection of critical information and through ineffective handling of legitimate export licensing cases. The minority staff has made preliminary findings that the technology transfer programs of the Department of Defense and the intelligence community contain basic deficiencies which impair the government's overall effort to control the flow of critical American technology.

RECOMMENDATIONS TO THE DEFENSE DEPARTMENT

Regarding the Defense Department, Fry said, the staff's findings were as follows:

1. The Freedom of Information Act is available to U.S. citizens, foreigners and Soviet surrogates to obtain critical dual-use technology. Dual-use technology should be excluded from FOIA requests.

2. The Defense Department has prematurely declassified sensitive data in accordance with an automatic declassification schedule. In other instances, critical technologies with military significance have not been classified. In both cases, the end result has been that sensitive information has been made available to anyone. There should be improved methods to determine whether information should be classified, declassified or remain classified.

3. On August 26, 1977, the Secretary of Defense issued an interim policy statement on export control. There has never been a followup to the interim policy, a reflection of the diminished priority afforded technology transfer throughout the executive branch. There is uncertainty regarding which DOD office has overall accountability for technology transfer decisions, causing unnecessary and costly delays in the resolution of export license reviews and resulting in the approval of exports not in national security interests. On May 19, 1979, the Deputy Secretary of Defense issued a directive spelling out specific areas of responsibility within the Department of Defense. Defense Research and Engineering (DR&E) was designated as the responsible office for technological matters and processing and coordination of export requests. It was also designated to serve as the DOD focal point on all aspects of export technology with the Department of State and other agencies. The Office of International Security Policy was to be responsible for policy and political considerations. The directive stated that disagreements between the two offices were to be resolved by the Deputy Secretary. Neither office has assumed overall accountability. There have been instances in which DR&E has made decisions on policy. In other instances, ISP did. There has been inadequate coordination and communication between the two offices.

4. In its technology transfer mission, DR&E does not have an adequate number of permanent staff specialists. Turnover of personnel is too high. Valuable time and resources are lost training new employees.

5. Military and DOD research facilities which review licensing cases lack a charter spelling out their export control responsibilities; and lack specific funding for this mission.

6. There is no adequate data base of information available to all participants in DOD's technology transfer programs. "This deficiency is analogous to prosecutors working without the benefit of a legal library," Fry said. There should be a centralized repository of information on data relevant to export license requests. Much of what is known about technology transfer lies solely in the minds of DOD personnel who work in this field. The result is inconsistent policy. One DOD research facility can review an export license case and raise no objection. Another DOD laboratory may receive a similar case and deny the export. A mechanism is needed to consolidate all available data.

7. The Defense Department does not review a sufficient number of free world export license cases. Frequently exports to free world nations are reexported improperly or illegally or diverted to Soviet Bloc nations. This was demonstrated in recent export violations involving Switzerland and West Germany which were used as transshipment points for the illegal reexport of high technology items to the Soviet Union. The United States trades with India and Pakistan and other nations which have open trade policies with the Soviet Union. It is unwise to export critical technologies to any nation without the benefit of DOD review.

8. DR&E has not devoted sufficient resources to reviewing foreign technical visitor programs. DR&E is unable to assess what subjects visitors are concerned with and what technology is being obtained. There is no way to measure what critical technologies might be obtained by visitors from hostile nations, thereby making it impossible for intelligence agencies to anticipate probable attempted acquisitions or to determine how a reported loss affects national security.

RECOMMENDATIONS TO INTELLIGENCE AGENCIES

Subcommittee investigator Glenn Fry went on to say that the effective control of critical dual-use technology is dependent on the gathering, dissemination, analysis and use of intelligence. He said the view of the minority staff is that the Soviets are precise about what technology they want from the United States. If the United States can determine what the Soviets want, this country will have strengthened its ability to prevent them from obtaining the desired technology. But intelligence efforts have not been adequate, Fry said, adding:

> Coordination among affected agencies is inadequate. Commitment of needed resources is lacking. The intelligence community is not organized to use information to block prohibited diversions.

In the intelligence field, Fry said, the staff had these additional findings:

1. The Export Administration Act mandated the Commerce Department to determine the foreign availability of critical dual-use technologies. The foreign availability of technologies is an important ingredient in the decision to license. But foreign availability determinations are not adequate.

2. Sources within the intelligence agencies informed the subcommittee staff that they have little communication with the Compliance Division of Commerce regarding on-going cases. One intelligence agency official told the staff there is little response from Commerce regarding what use is made of the information it receives. The information is submitted to the Office of Intelligence Operations in the Commerce Department. It is not known whether the data is sent to the Compliance Division and to licensing officers. The Compliance Division rarely seeks the expertise of the intelligence community.

3. Methods should be devised that enable sensitive information to be sanitized and passed on to law enforcement personnel. Several experienced law enforcement officers told the staff that frequently intelligence on technology transfers has such a high classification that many

agents working on export control cases cannot see it because their clearances are too low.

4. The Defense Intelligence Agency conducts end-user investigations by determining whether the end use of an export is in the national security interest. If it is to carry out this function effectively, DIA should receive additional resources.

5. The executive branch has no mechanism for evaluating what information has been lost. There is no system for following up investigations of questionable exports or reexports. There is no system to determine what has been exported or reexported or where and how it was used. There is no way to determine the adverse impact to the U.S. of dual-use technology that has been obtained by the Soviet Bloc.

6. The government should form a high level interagency task force comprised of senior Cabinet-level officials to address the problem of export control.

V. IG Report Corroborated Much of Subcommittee Staff Critique

The subcommittee hearings on technology diversions ended on May 12, 1982. A month earlier—on April 13—the Inspector General in the Commerce Department, Sherman M. Funk, began his own examination of the effectiveness of the Compliance Division. Funk assigned to the task his Assistant Inspector General for Investigations, Michael M. Ryman, two criminal investigators, two auditors and a management analyst. The Commerce Department gave the subcommittee a copy of the Inspector General's report of its inspection on July 16. The report, along with the Department's response to the IG's findings and recommendations, was printed in full in the hearing record.

Many of the assertions made in the subcommittee staff's critique of the Compliance Division were corroborated by the IG inspection team. The IG's report said, for example, that there is "a widespread perception" that the Commerce Department has made an inadequate commitment of resources and moral support to the task of controlling U.S. technology exports because the Department places a high priority on the promotion of trade. The report said:

> Many of the problems highlighted in this report have been identified in earlier reviews provided to (the Commerce Department) management. The Department of Commerce has failed to correct these problems despite strong public statements by the present and past administrations in support of tight controls over the export of high and dual-use technologies. This failure raises serious questions about the Department's commitment to, and ability to enforce, the Export Administration Act of 1979.
>
> The IG inspection team repeatedly was advised that the problems it noted reflected the Department's dual and possibly conflicting missions of trade promotion and export control. The team was not able to reach this conclusion unequivocally. It is clear, however, that the Department's failure to provide adequate resources, policy guidance and management direction has impeded the compliance effort and produced at very least the perception of a de facto supremacy of trade promotion mission over the Department's export control function.
>
> What is also clear. from the findings in this report. is that the Department of Commerce has not taken a bold lead in forging an aggressive multi-agency effort to halt the illicit export of controlled products.

Other findings by the Inspector General's Office included these:

1. A policy that restricted travel by Compliance Division investigators led to a situation in which most inquiries were made by telephone or mail. Necessary field inquiry rarely took place. "Examples

of lost opportunities for enforcement and prosecution of export control violations are not difficult to find," the report noted, citing one recent case in which a Compliance Division agent's request for travel was denied, thereby precluding his ability to go forward with a thorough inquiry and, in effect, permitting a consortium of companies to continue their illegal export of high technology products to the U.S.S.R. and the Soviet Bloc. Another agent's request for travel to the West Coast was denied despite substantial evidence of unlicensed shipments of microchips and other restricted items. Such travel restrictions, the IG report said, have "allowed continued criminal activity and nonenforcement of the export laws."

2. The Compliance Division frequently hired inexperienced investigators and provided no training for agents once hired. In one instance, the Division hired an untrained and inexperienced agent, who was then allowed to conduct official investigations for the next 6 months without an investigator's credentials. Noting that hiring untrained, inexperienced agents for this kind of investigative work is in violation of Office of Personnel Management rules, the IG report said that the training offered Compliance Division members in fiscal year 1980 was limited to a report writing course for the Chief of Investigations Branch. Financial records showed a total expenditure of $24.98 for training of agents in fiscal year 1981, and no expenditures at all in fiscal year 1982.

3. The Compliance Division was found to be bereft of the technical equipment required to collect criminal evidence. The Division borrowed from other Federal agencies equipment such as cameras, surveillance team communications gear, consensual monitoring devices and other law enforcement aids. Funds earmarked for the purchase of technical equipment were used to buy office machinery and furniture.

4. The Compliance Division's Intelligence Branch has not developed its own intelligence leads on potential export violators; nor has it solicited such leads from the U.S. Government's intelligence community. Lacking sufficient manpower and expertise, the Intelligence Branch regularly failed to use critical export information already available to it. "An efficient and effective intelligence operation cannot be conducted in such a manner," the IG report said, adding that the Commerce Department should be directing and soliciting a steady flow of information with the U.S. intelligence organizations to identify targets, patterns and sources of controlled technology leakage. In a recent 6-month period, less than 15 percent of the leads referred to the Intelligence Branch were checked out and hundreds of leads from prior years have gone untouched. The IG report added:

> A large backlog in the Intelligence Branch slows the investigative process since most investigations are not started without the intelligence referral. Furthermore, the backlog puts undue pressure on the small staff in the Intelligence Branch to cut short their intelligence analyses, close cases prematurely, or forego further information gathering from the intelligence community or other sources.

5. Cooperation and coordination between the Compliance Division and the U.S. Customs Service has not been good and adversely affected enforcement of the export laws. The IG report said there had been efforts by some Compliance Division personnel to prevent coordination with Customs. Also cited were incidents of "interagency hostility"

and "investigatitve case inteference" by both Compliance and Customs representatives. A source of conflict was the Commerce Department's interpretation of section 12(C) of the Export Administration Act of 1979. The Department interpreted this provision to mean that only the Secretary of Commerce could authorize the release of proprietary information to the Customs Service, the FBI and other law enforcement entities.

6. Traditional law enforcement organizations have an agent's manual which is given to each investigator so that he is informed as to the policies and procedures of his unit. The agent's manual for the Compliance Division is "nonexistent or outdated and not widely disseminated to staff members." Despite its inadequacies, the document is classified at a level above that of most Compliance Division agents. "Considering the present lack of training provided new investigators," the IG report said, a current and readily available agent's manual "is an absolute necessity."

7. The Inspector General found that the Compliance Division's working space in Commerce Department headquarters in Washington is "crowded, poorly equipped, ill maintained and noisy" and provides agents no privacy for confidential meetings and interviews with informants.

8. The IG report directed sharp criticism at Bohdan Denysyk, the Deputy Assistant Secretary for Export Administration, who was accused of improperly interceding in Compliance Division investigations with the result that his conduct denigrated the Division's established chain of command and management as well as creating "multiple sources of concurrent supervisory instruction" to Compliance Division agents. This caused an obstacle to the "efficient and effective operation" of the Division. The report added that in this conduct Denysyk was assisted by Vincent F. DeCain, Acting Director of the Office of Export Administration. Organizationally, the Compliance Division resided within the Office of Export Administration and the OEA was under the Deputy Assistant Secretary for Export Administration. The IG report said that Denysyk could have worked to improve the Compliance Division but instead chose to circumvent the Division and established procedures and pursue investigations without the participation of appropriate Compliance Division managers. Denysyk, the IG report said, "apparently prefers to use 'favorite son' investigators and a paid consultant to manage and conduct investigations."

Denysyk was accused of personally intervening and conducting crucial aspects of sensitive investigations in seven separate Compliance Division cases. The report said it was particularly undesirable for Denysyk to intercede in criminal inquiry because Denysyk "himself is neither a trained investigator nor has any background in criminal investigation."

Denysyk's reported insertion of an outside consultant into the affairs of the Compliance Division also came under fire. Bohdan Denysyk, the IG report said, weakened the Compliance Division by shifting part of its duties to the consultant and a Departmental task force and by excluding the Division itself from involvement in certain actions taken by the consultant. Denysyk "misused his expert/consultant whom he hired ostensibly to evaluate and upgrade the Compliance Division." The report went on to say:

> Personnel regulations have been violated, as well as sound management practices, by interjecting this consultant in an operating role for which he has little expertise.

Because the consultant operated outside the Compliance Division and had to adhere to limited standard operating procedures, reporting directly to Denysyk, the Inspector General's report questioned the "legality and propriety" of his employment. Chapter 304 of the Federal Personnel Manual says that improper employment of experts and consultants is illegal and "wasteful and destroys the morale of career specialists." The report added:

> One of the manual examples of improper employment of an expert is assignment to a noncritical, nonsensitive position which could be handled as well by a regular Federal employee. Such a violation seems to have been made in this case. Financial compensation—$93 per day—for this fulltime position may also have been made to avoid competitive employment procedures and General Schedule pay limits.

Stating the Commerce Department's responses to the IG report, Lionel H. Olmer, the Under Secretary for International Trade, said the report focused on problems that "are soon to be things of the past or already are." In a July 2, 1982 memorandum to Inspector General Sherman Funk, Olmer said the Department's Export Administration Act enforcement function was in the process of undergoing a major reorganization.

As for the specific findings of the IG report, Olmer agreed with much of what the report stated. However, he asserted frequently that, while the shortcomings described by the IG had existed in the past, corrective action was being taken and that by the end of 1982, "we will have a very positive story to tell" in describing the reforms that will have been put into place by then.

With reference to the IG report assertions about the reportedly questionable conduct by Deputy Assistant Secretary Bohdan Denysyk and his hiring and use of a consultant, Olmer said Denysyk denied having interceded in the daily activities of the Compliance Division. The Acting Director of the Office of Export Administration, Vincent DeCain, also denied the charge. However, Olmer said, Denysyk tried on occasion to gather information about how the Division was getting along. Olmer said this conduct was—

> . . . solely for the purpose of enlisting the cooperation of concerned foreign governments in paving the way for Compliance Division . . . investigators. Their respective conduct in these cases was entirely proper and consistent with the practices of other law enforcement agencies whose senior officials often take initiatives to enlist the cooperation of their senior foreign government counterparts in paving the way for U.S. agency investigators.

Olmer acknowledged that Denysyk's consultant had gone beyond the terms of his job description. Action had been taken to confine the consultant's activities to 'the terms of his employment and appropriate security regulations," Olmer said in a reference to the IG's assertion that the consultant had been shown documents he was not cleared to see.

VI. Witnesses Offered Recommendations To Improve Export Control Capability

CUSTOMS COMMISSIONER OPPOSED ENLARGING COMPLIANCE DIVISION

Witnesses from government and the private sector generally tended to support the finding of the subcommittee minority staff that reform is called for in the manner in which the executive branch controls exports. For example, William Von Raab, the Commissioner of Customs, testified that he felt, from an enforcement point of view, that the Compliance Division in the Commerce Department was too small to carry out the investigative responsibilities of the Export Administration Act. Von Raab said the enforcement function could be executed in a more comprehensive, effective manner by Customs. He said that if Customs were given total responsibility for investigating alleged violations of the statute, his special agents and inspectors would rely on, and work closely with, Commerce Department export licensing personnel.

Von Raab said that if Customs were given the responsibility, it could carry it out without hiring new personnel but would instead rely on current manpower levels. Unlike the Commerce Department which has committed approximately 11 investigators, 3 to 5 intelligence analysts, and 5 or 6 inspectors to enforce export controls, Customs currently has 125 inspectors, 50 special agents and 25 support personnel working exclusively on export cases under Project Exodus, a recently begun national enforcement program "aimed at combating the trafficking in illegal exports," Von Raab said, adding that Exodus already had realized encouraging results. In addition to the personnel assigned to Exodus, Customs can also call upon its 5,000 other inspectors and 600 special agents in export cases, Von Raab said. Moreover, he said, Customs has attachés in many nations and mutual assistance agreements with Canada, France, Austria, Mexico, and West Germany. In addition, Customs personnel have traditional law enforcement tools such as the authority to carry firearms and make arrests, he said.

One of the findings of the subcommittee staff was that tension had existed between Customs and the Compliance Division of the Commerce Department, resulting in reduced cooperation and diminished effectiveness in investigations. Von Raab acknowledged that there had been such problems in the past but that he and Lawrence J. Brady, the Assistant Secretary of Commerce for Trade Administration, had made it their "personal campaign to improve the cooperation of the two services and particularly to improve the Commerce Department with respect to our activities." Von Raab went on to say:

> I believe that he (Brady) made a number of changes within the Commerce Department. He is trying very hard. It takes a long time to turn around a bureaucracy like the Commerce

Department. I, fortunately, am lucky enough to have an enforcement organization who are extremely dedicated individuals and, therefore, we have been able to respond to Exodus quickly.

But I would like to indicate that the environment between Commerce and the Customs Service has improved immeasurably. And I have great hopes for the developing relationship.

The subcommittee staff had cited a 1980 memorandum written by a senior Customs Service official who said that the Compliance Division was intruding into legitimate Customs activities overseas and, in so doing, was running the risk of compromising investigations, negating longtime positive relationships with foreign governments and undermining U.S. national security. Asked about the memorandum, Von Raab said he had not seen it, but he did say:

> . . . I do believe there are problems with Commerce conducting certain foreign investigations. Customs does have much better connections with the (overseas) police agencies that these investigations would typically use . . .
>
> . . . it is a real problem for Commerce abroad in my opinion. Occasionally we stumble over each other but I think the bigger problem is that the police organizations don't like the Commerce attachés.

Asked if Customs should be given the entire enforcement function under the Export Administration Act, Von Raab said Customs should have "the major share, the 95 percent," but he would support the continued existence of the Compliance Division in the Commerce Department, although he added, "I would not suggest that they need to increase their forces in any way."

In advocating that the Compliance Division be abolished, the subcommittee staff said that the mere existence of the Division was an impediment to effective enforcement of the Export Administration Act. Incapable of doing an effective job, the Compliance Division, as long as it existed, would prevent other law enforcement entities from taking over the function, the subcommittee staff said.

Von Raab did not agree with the subcommittee staff. But testifying with him were two senior Customs officials who did not agree with Von Raab. George G. Corcoran, Assistant Commissioner for Border Operations, and Patrick O'Brien, Director of General Investigations, both said the Compliance Division should not have the enforcement function, that this duty should reside in Customs and that Commerce should retain its licensing responsibilities. O'Brien, in fact, said he thought the enforcement function should be separate from licensing. A similar arrangement currently exists in connection with the Arms Export Control Act. The Department of State administers the statute and has licensing duties while the Customs Service investigates alleged violations.

Turning to Von Raab, Senator Nunn reminded the Commissioner that, while he had testified that he favored keeping the Compliance Division in existence, he had recommended against enlarging the Division. Senator Nunn asked:

> What you are basically saying is we should leave some authority and maybe a few people in the Commerce Department for sensitivity and prestige purposes and then shift the main responsibility to the Customs Service?
>
> "That is probably true," Von Raab replied.

SHIFT IN ENFORCEMENT STRATEGY WAS PROPOSED BY COMPUTER BUSINESSMAN

On the subject of controlling technology transfers, the government is placing its enforcement focus on the wrong end of the export spectrum. Too much emphasis is placed at the border. But today's technology is too small to be detected at the point of exit. It would be wiser to concentrate at the source; that is, at the plants and factories that develop and produce high technology. A comprehensive education program, aimed at alerting the business community to the problem of technology transfer, would pay greater dividends than continued preoccupation with the border.

That view of how the U.S. could improve its enforcement of export controls was given the subcommittee by Charles P. Lecht, former president and chairman of the board of Advanced Computer Techniques Corporation of New York.

Lecht said that, while the education program he advocates would be a good idea, he has never seen government try to carry out anything like it. He testified that he rarely received any information from government on export controls—and what he did see was out of date.

Lecht said government efforts to control technology exports will continue to fail because too few resources are devoted to communicating with industry. Modern technology is too easily smuggled and too readily available throughout the world for the U.S. to try to keep certain items out of the reach of the Soviet Union.

Lecht said the government education program should acquaint producers with the technology transfer problem and encourage them to cooperate with authorities in controlling it. He said that neither the Commerce Department nor any other component of government has brought the message home to businesses as to what they can sell legally to the Soviets and what they cannot.

American high technology businessmen do not have much confidence in export controls, and are annoyed because they see foreigners sell items to the Soviet Bloc that U.S. firms are not supposed to sell them. Lecht said. The French, English, Italians and the overseas offices of certain American-based conglomerates trade in high technology equipment with the Soviet Bloc. He explained:

> . . . abroad I am afraid our partners don't have the same sense of urgency with regard to the handling of our high tech products.

Lecht, whose company had extensive business dealings in Yugoslavia, said that he had been approached there by Russian military officers and asked to provide technical information but that he had refused. He said that his impression of Soviet interest in U.S. high tech-

nology was that the Russians were not trying to copy, imitate or use it—but instead wanted to understand American military weapons so that they could destroy or immobilize them more readily in the event of war. Lecht said:

> . . . they have for the most part chosen to selectively target and secure those areas of American technology which are critical to the secrets of our military defense. They need to know such things as when and where our missiles and planes take off and how to jam the electronics in these. As long as the United States fails to recognize the bases and nature of their strategy and persists in outmoded, ineffective and unfocused attempts to control the export and transfer of technology, the Soviets will, I am afraid, find their global task that much simpler.

FBI EMBARKED ON BUSINESS EDUCATION PROGRAM

Lecht testified that government efforts to control technology exports would be improved if the producers of this equipment were made the targets of an education program, alerting them to the problem and asking them for their help. Members of the subcommittee were supportive of that idea.

According to Edward J. O'Malley, chief of the FBI's counterintelligence section, the Bureau has embarked on such an education program in the defense industry. Called DECA—for Development of Counterintelligence Awareness—the program is designed to inform the Nation's 11,000 defense-related companies involved in classified contracts about the "threat posed by activities of the hostile intelligence services," O'Malley said.

Personal contact had been made with 6,000 firms, and each FBI field office now has at least one special agent whose responsibilities include contact with companies that potentially could be earmarked for Soviet technology acquisition efforts.

O'Malley said the FBI can become involved in export control cases in several ways. If the technology is classified for national security purposes, the Bureau will investigate on the basis of the espionage statutes. If unclassified technology valued at more than $5,000 is stolen and transferred across State lines, the FBI can investigate under the Interstate Transportation of Stolen Property statute.

While export cases concerning non-classified technology under the Export Administration Act are outside the FBI's jurisdiction, O'Malley said that if there is involvement by a foreign intelligence agency the Bureau will investigate. Even if there is no readily apparent hostile intelligence involvement, the FBI still will be interested because it is likely that somewhere in the transaction a foreign spy connection will turn up.

With regard to the Export Administration Act and the statute's enforcement arm, the Compliance Division of the Commerce Department, the subcommittee wanted to know if the FBI had a cooperative working relationship with Compliance and how many cases the Division had referred to the Bureau. O'Malley said the FBI had "an excellent day-to-day relationship" with the Compliance Division, but that

in the past 12 months the Division had not referred a single case to the FBI.

Conversely, O'Malley said, the FBI and the Customs Service made frequent referrals of criminal cases to one another. Pointing out that the FBI also had a "very close working relationship with Customs," O'Malley added:

> At the current time we have a number of very . . . substantial cases that we are working jointly with Customs in the technology area.

In the subcommittee staff's evaluation of the Compliance Division, it was noted that a source of the tension between Customs and the Division was the Commerce Department's strict interpretation of the proprietary aspect of the Export Administration Act, section 12–C. According to the Commerce Department's interpretation of 12–C, no export information can be turned over to Customs without the question being decided by the Secretary of Commerce, a procedure that, in effect, either precluded Customs from seeing the requested data, or caused such long delays that it had a detrimental effect on the investigation. According to O'Malley, the FBI had the same problem with Commerce over section 12–C.

O'Malley said the Export Administration Act required the Commerce Department to obtain the Secretary's OK before making public export licensing data. O'Malley said the Commerce Department's interpretation of the statute is that "making it public is synonymous to giving it to other agencies within the Federal Government."

The Office of Legal Counsel in the Justice Department objected to the Commerce Department's interpretation of the law, communicated its objection to Commerce in writing and there now has been an agreement whereby in the future licensing data will be shared with the FBI without having to obtain the Commerce Secretary's approval, O'Malley said.

Just as he said the Commerce Department had not referred any criminal cases to the FBI in the last year, O'Malley also testified that the Bureau had not worked on an inquiry jointly with the Compliance Division in a year. Senator Nunn asked why there were no referrals and no joint cases. O'Malley replied:

> I think it is probably because in the past Commerce has been understaffed. They do not have, compared to Customs, the number of investigators out in the field or the people with the same kind of law enforcement training, that people in the field in terms of Customs would have. We have a tradition which transcends the technology transfer issue of working very closely with Customs. They have a large presence . . . throughout the country (at) all the key ports. So I think these are the general reasons why we exchange information more frequently with Customs than we do with Commerce.

Senator Nunn asked if the Compliance Division were capable of enforcing the Export Administration Act. O'Malley referred again to the lack of personnel in the Division and their lack of training and the fact that they are not stationed throughout the Nation or abroad. Because of these deficiencies, there were, he said, only two choices—

> . . . either increase or improve the capabilities of Commerce in the areas that I mentioned or consider transferring it to another agency.

Senator Nunn asked if the Customs Service could do a better job of enforcing the Export Administration Act. O'Malley said:

> . . . Customs does have a larger presence, both here in the United States and abroad. Their training is better. They have law enforcement powers which Commerce people do not have.

FBI Director William Webster, who did not testify at the hearings but whose January 15, 1982 speech before the Electronic Industries Association in Boca Raton, Florida, was received as Exhibit No. 38, said the Bureau's responsibilities in the counterintelligence-export control areas have grown at the same time its resources have been reduced. He said that last year more than 82,000 persons from the Soviet Union and Soviet Bloc—sailors, tourists, trade mission personnel and diplomats—entered the U.S. But, compared to 1976, the FBI today has about 10 percent fewer agents.

". . . our budget isn't keeping pace with inflation," Webster said, "yet our foreign counterintelligence assignment continues to grow both in scope and importance." Webster also noted that 3,500 commercial visitors and 30,000 tourists and immigrants who came to the U.S. from mainland China and the 130,000 immigrants who arrived from Cuba in 1980. Most of the Russian, Soviet Bloc, Chinese and Cuban arrivals were here for legal pursuits, Webster said, but some must be assumed to have come to collect sensitive information and the FBI's task of countering their efforts "is becoming increasingly difficult."

FREEDOM OF INFORMATION ACT CAUSES PROBLEMS FOR DEFENSE DEPARTMENT

Presiding over the Pentagon's massive unclassified information-dispensing apparatus, Arthur F. Van Cook has a unique position from which to observe the efforts by the Soviet Union to obtain through legal means American military technology.

Van Cook, Director for Information Security in the Department of Defense, told the subcommittee that the Soviets apparently obtain all the technical publications issued by the Pentagon and, through surrogates and the Freedom of Information Act, acquire many more military documents not readily available to the American public.

As a demonstration of how accommodating the Pentagon has become for persons seeking unclassified military data, Van Cook quoted a Soviet scientist, who had defected to the West, who said that the majority of Soviet information requirements can be obtained openly in the U.S. The FBI made a similar estimate, Van Cook said, as he explained:

> The Department of Defense has been concerned for some time about the virtual unremitting flow of unclassified defense information to our adversaries. This hemorrhage of information to hostile nations, particularly technology and technical data with military applications, is one of the more serious problems confronting the Department.

Asserting that the Defense Department consistently has supported the 30-year trend toward more "openness in government," Van Cook said Pentagon policy is to inform the public fully about the "activities and operating functions" of the armed services. However, he said, the openness policy may have gone too far in certain instances.

Van Cook said that until February of 1980, the Soviets were able to purchase every one of the 80,000 technical documents issued each year by the Commerce Department's National Technical Information Service [NTIS]. The U.S.S.R.'s subscription was canceled following the invasion of Afghanistan but the Soviets still have access to NTIS because Soviet Bloc nations may still subscribe.

The "damage" standard—that is, will public disclosure of this military data "damage" national security?—allows for the declassification of militarily critical information that can make the Soviets more competent technically and, therefore, strengthen their armed forces. Van Cook said, for example, that, on its face, the declassification of certain technical characteristics of the electronic components in an American missile guidance system may not appear to damage national security. But that data, in the hands of the Soviets, may enable them to improve their own guidance system.

Moreover, once the information about the U.S. missile's electronic components is declassified, Van Cook said, it becomes vulnerable to a Freedom of Information Act [FOIA] request, unless it can be shown to be exempt from the statute. All too often an exemption to FOIA cannot be established and the data must be released.

Triggering the release of such militarily critical information has been a new "cottage industry" that has sprung up in response to FOIA, Van Cook said, pointing out that companies have been formed whose sole objective is to obtain technical information from the government through FOIA and then sell it in the U.S. and abroad.

FOIA requests can be filed by anyone—whether or not an American citizen from the U.S. or from abroad—and they must be treated the same. One FOIA request was received from a Norwegian "access professional" who, at the time he sent it in, was on trial in Norway for espionage.

Such requests were a source of concern to Van Cook. Under questioning from Senator Nunn, Van Cook said felons, incarcerated convicts, spies and Communist dictators are no different than law-abiding American citizens when it comes to FOIA requests. If they ask for an unclassified military document, the Defense Department is obliged to give it to them, unless it falls into one of nine exempt categories, none of which has anything to do with the integrity or nationality of the requestor. The following exchange occurred between Senator Nunn and Van Cook:

> Senator NUNN. We are saying right now if Fidel Castro wrote in to the Department of Defense and said he wanted 200 items that were unclassified that you would have to send them to him?
>
> VAN COOK. That is correct, sir.
> Senator NUNN. Qaddafi in Libya. Is that correct?
> VAN COOK. That is right.
> Senator NUNN. The Ayatollah of Iran?
> VAN COOK. Yes, sir.

Senator NUNN. Don't you think on the face of it, that is ludicrous?

VAN COOK. Yes, sir, I do.

In the so-called "Florence case," [7] a court ruled that FOIA required the Defense Department to honor a request to disclose a certain index of the titles of specific technical military reports. The index itself was classified but the items in it were unclassified. Van Cook said the confidential classification was based on the premise that the compilation of the data would serve to strengthen another nation's military prowess. Van Cook said the court ordered release of the index because FOIA stipulated that "any reasonable segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt."

As chairman of a DOD working group on technology transfer, Van Cook said he participated in the drafting of a proposal to amend FOIA by exempting from disclosure technical data which cannot be exported without a Commerce Department validated export license. The proposal was put forward because FOIA contains no exemption regarding technical data. However, Van Cook said, FOIA does have a provision saying that another statute precluding release of the requested information could prohibit disclosure. But the provision is not precise enough and might not apply if the request were drafted to circumvent it. The amendment to FOIA was drafted to clarify the law.

Another proposal that emerged from the working group would have authorized the Secretary of Defense to classify at a level lower than confidential information which might compromise this Nation's military advantage. Van Cook said the proposal did not receive "broad executive branch support" and was dropped.

A new computerized system for keeping track of all disclosures of military critical information was placed into operation in May of 1982, Van Cook said. Known as FORDTIS—Foreign and Technical Information System—the automated data base is designed to give Federal agencies involved in technology transfer prompt and comprehensive information on the export of munitions and technology.

BUCKLEY AND BRYEN STRESSED NEED TO ENLIST ASSISTANCE FROM ALLIES

Testifying on behalf of the Defense Department, Michael Lorenzo, Deputy Under Secretary of Defense for Research and Engineering, told the subcommittee of the Department's program to maintain a Military Critical Technology List [MCTL] and other sources of information to guide officials in making export control decisions. He said DOD had begun a training program for Customs Service personnel to "raise the batting average of Customs in detaining illegal shipments."

Another Defense spokesman—Dr. Stephen D. Bryen, Deputy Assistant Secretary for International Economic, Trade and Security Policy—told the subcommittee that America's NATO allies had made export control policy in the past without the participation of their military ministries. He said that except for the U.S. and one or two other countries, defense ministries abroad play little or no role in

[7] *William G. Florence* v. *U.S. Department of Defense, et al.*, civil action 75–1869, U.S. District Court, District of Columbia.

the review of strategic trade exports. DOD is encouraging foreign military officials to be included in such decisions.

Dr. Bryen cited a new NATO study on the security implications of transfer of military technology to the Soviet Bloc. This study is the first NATO review of the technology transfer issue, he said. DOD is working to generate more NATO interest in export controls.

However, he said, many problems remain at DOD such as the lack of a centralized data base on technology transfer. "This committee should know," Dr. Bryen said, "that on taking office there were no coherent records available on past DOD determinations; nor was there any single source to appraise the results of past activity."

Lawrence J. Brady, the Assistant Secretary of Commerce for International Trade, testified that at the Ottawa Summit in July of 1981, President Reagan made a personal appeal to the leaders of Western Europe, Canada and Japan to work with the U.S. in taking steps to blunt the Soviet raid on Western technology. As a result of the President's action, the first high level meeting in 25 years of the Coordinating Committee (COCOM)—Japan and NATO nations except Iceland—was held in January of 1982 to improve export controls on high technology.

COCOM—The Western Democracies' export control organization—was one of the subjects discussed by James L. Buckley, the Under Secretary of State for Security Assistance, Science and Technology, in his testimony before the subcommittee.

COCOM, whose sanctions on export controls are voluntary, is charged with making lists of commodities embargoed for export to the Soviet Union, Soviet Bloc, China and other Communist countries in Asia; and with ruling on exceptions. In deciding on a nation's request to export an item on the embargoed list, COCOM "works on the principle of unanimity," Buckley said, pointing out that in its 30 years of existence there had been very few cases in which a government had exercised its sovereign right to sell something COCOM objected to.

During the 1970s—in what he called "the honeymoon days of détente"—the U.S. went from being the least frequent petitioner for exemptions to being the most frequent. He added, "We now know that was a mistake."

The Department of State has the responsibility for administering the Arms Export Control Act. The Department issues licenses under the statute. Enforcement is carried out by the U.S. Customs Service. Buckley said the State Department is satisfied with the arrangements with Customs and described the relationship between the two agencies as being "excellent."

Buckley said Customs' enforcement of the statute made good sense from an organizational point of view. Citing the fact that Customs has 600 special agents assigned to 58 U.S. ports and has formal ties to 87 other nations through the Customs Cooperation Council, Buckley said:

> The Customs Service has a longstanding and well-established presence at the ports of the United States. The Service is so organized that the performance of the function fits in with its other responsibilities at the ports. The alternative would appear to be the establishment of a second organization at the ports solely for the purpose of processing the export of defense services. In our judgment, this would be redundant, extravagant and wasteful.

INTENTIONAL
BLANK

VII. Findings, Conclusions, and Recommendations

This report is based on the subcommittee's investigation and hearings into the effectiveness of the executive branch in enforcing export controls, particularly with reference to the transfer of technology to the Soviet Union and Soviet Bloc. The subcommittee has special interest in evaluating the government's response to the all-out campaign of the Soviet Union to acquire Western technology.

The dimensions of the Soviets' technology acquisition drive were outlined in the CIA report which was prepared to respond to this subcommittee's investigation. The CIA report described the Soviet Union's campaign to acquire Western technology as being massive, well planned and well managed—a national program approved at the highest party and governmental levels. The CIA report concluded:

> Stopping the Soviets' extensive acquisition of military-related Western technology—in ways that are both effective and appropriate in our open society—is one of the most complex and urgent issues facing the Free World today.

The subcommittee shares with the CIA that concern. Not only must the Soviets' extensive acquisition effort be blunted, effective action is called for promptly. Unfortunately, priceless U.S. technology already has found its way to Moscow. Advanced American microelectronics, laser, radar and precision manufacturing technologies have been obtained by the Soviets and have enabled them to make giant strides in military strength at a minimum of risk, investment and resources.

If the Soviet Union were applying Western technology to the objective of increasing its capacity to produce more consumer products, the threat from their acquisition drive would be less serious. However, the evidence is strong that virtually all the technology they obtain from the West is applied to the Soviet military industry. The military buildup in the Soviet Union is going forward at a rapid pace. Consumer needs take a back seat to armaments. As one former Soviet engineer told the subcommittee, the Soviet industrial capacity is so overburdened with military production that the Soviets could not make a civilian or commercial application of certain high technology products even if they wanted to. It is hoped—for the sake of the Soviet people, for the sake of world peace—that the Soviet military buildup will subside. In the meantime, however, there is no reason why the West should contribute, by weak export controls, to the Soviet Union's technological needs.

The subcommittee makes the following findings and recommendations as a result of the investigation and hearings:

Intelligence and Technical Evaluation

(1) The Soviets dedicate substantial resources to highly focused attempts to secure American technology. They are becoming increasingly adept in that effort. By contrast, the American response often has been

unorganized. A restructuring of American efforts to halt undesired technology transfer is called for. Through improved intelligence, the government must determine what it is that the Soviets want and then model its response accordingly. In other words, we must diagnose precisely the nature of current Soviet needs for our technology.

Frequently, the assertion was made at the hearings that the U.S. may be trying to control too many commodities—and, because it tries to do too much, the government ends up controlling too few goods. Through improved intelligence, the government can learn more precisely what the Soviets want and need. The government could reduce the number of controlled items—and could do a better job of preventing the Soviets from obtaining the commodities they desire most. Improved intelligence, coupled with an improved system for conveying that intelligence in a sanitized form to law enforcement, would constitute a stronger export control mechanism.

(2) Congress should consider establishing a center for technical expertise to be located at a National Laboratory whose purpose would be (1) to provide technical evaluation on export cases too complex for routine licensing applications; and (2) to conduct research into technical questions related to export matters. The center, which would be staffed by about 20 experts from a variety of scientific disciplines in the national security field, would provide technical guidance to licensing officers and to Federal agencies involved in export controls. The existence of the center, and the high-level technical assistance it would provide other agencies, would enable other components of government involved in export control cases the opportunity to concentrate their evaluation efforts on policy and policy-related matters and limit the amount of time they would have to devote to strict baseline technical assessment.

Conversely, such a center would enable experts to make technical evaluations free from the influence of policymakers. Dr. Lara Baker, a computer scientist with experience in the intelligence field, testified about the need for such a center and estimated that the cost of the facility would be about $5 million a year, an amount, he said, which represents a very small fraction of the value of the technology currently at risk.

(3) The Export Administration Act of 1979 gives primary responsibility to the Commerce Department to determine the foreign availability of dual-use technology. This is an important responsibility. It is essential that licensing officers know what equipment can be purchased overseas. In many cases, it is unfair to preclude American industry from exporting equipment which already is being sold abroad. The Commerce Department should review its own capabilities and resources in this regard. If the job is found to be being handled in an unsatisfactory manner, the Department should make every effort to take appropriate corrective action. A Defense Department official testified that DOD already is doing considerable work in connection with foreign availability. Because of the national security implications of the foreign availability issue, the Commerce Department should operate in close harmony with DOD in determining what is being sold overseas. Testimony at the hearings indicated that many businessmen resent export controls because they believe much of the equipment on the controlled list is available from foreign sources. The subcommittee

believes that cooperation and assistance from the private sector are necessary if export controls are to be enforced more effectively. By the same token, cooperation is a two-way street. The business community has a right to expect that, wherever appropriate, they should be entitled to compete on equal terms with foreign businesses. Export control decisions should be made with a view to allowing as much free trade as possible. Arbitrary or inconsistent lists of controlled goods are a severe disincentive to exporters seeking to establish markets overseas while simultaneously remaining reliable suppliers at home. Government should use the foreign availability issue as an opportunity to demonstrate that it is taking steps to improve its own management of the technology transfer problem.

(4) The Defense Department and the intelligence agencies should conduct a study to determine the technology lost to the Soviet Union and Soviet Bloc. A good start in that direction was the CIA report of April 1982 entitled, "Soviet Acquisition of Western Technology." The study should divide the technology losses according to subject areas such as (a) scientific and technical exchanges; (b) student exchange programs; (c) sales of advanced technology equipment and know-how; and (d) illegal acquisitions of U.S. technology or equipment. The study will be useful in assessing the impact on national security of these losses and in enabling law enforcement officials to anticipate the emerging technologies likely to be targeted by future Soviet acquisition efforts. The study also could identify those countries whose export control policies, coupled with their relationship with the U.S.S.R., indicate that they may be potential channels for unauthorized reexport of controlled high technology items.

In addition, information from the study would be the foundation for creation of a automated data base which can be used to make accurate, up-to-date and consistent licensing decisions and recommendations.

One important use of this data base will be to enable the affected agencies such as the Commerce and Defense Departments to evaluate export license applications in light of each country's previous record on diversions. The Senate Banking, Housing and Urban Affairs Committee, which has jurisdiction over the Export Administration Act, may wish to review the statute in terms of the possible need to enlarge the role of the Defense Department in reviewing Free World applications.

LAW ENFORCEMENT

(5) There is a need for reassessment of the ability of the Department of Commerce to carry out its present enforcement responsibilities under the Export Administration Act (50 U.S.C. App. 2401 et seq.). Commerce presently carries primary law enforcement responsibility, with secondary jurisdiction resting in the U.S. Customs Service. Commerce maintains both licensing and enforcement under the act; by contrast, under the Arms Export Control Act (22 U.S.C. 2751 et seq.), those functions are handled separately by the Department of State and the U.S. Customs Service.

Hearing evidence and a detailed staff investigation of the problem revealed a lack of traditional law enforcement capabilities at the Department of Commerce, including shortages in manpower, equipment,

fundamental law enforcement training and experience. The evidence strongly suggests that the Commerce Department to date has been unable to enforce the EAA controls in the face of mounting Soviet efforts to secure sensitive American technology.

In light of the testimony received at the hearings, some members of the subcommittee are of the opinion that current enforcement responsibilities should be altered by delegation of full enforcement responsibility to the U.S. Customs Service, with the licensing function remaining at the Commerce Department. Other members of the subcommittee feel that that decision should be temporarily delayed until it can be determined whether the Department's proffered improvements will adequately correct present enforcement problems.

In any event, the subcommittee will continue its interest in the Commerce Department's enforcement operation under the Export Administration Act. Undoubtedly individual members of the subcommittee will introduce legislation as a result of these hearings, reflecting their own views on reforms needed to enforce export controls more effectively.

(6) The Export Administration Act and the Arms Export Control Act should be amended to include as a criminal offense, the possession or attempted possession of restricted goods with the intent to export such goods unlawfully.

Hearing evidence established the many difficulties law enforcement authorities encounter in the prosecution and investigation of export offenses. One problem lies in the absence of any offense until a suspect actually "exports" the goods in question. When arrest is delayed until the moment of export, law enforcement necessarily risks the loss of territorial jurisdiction if the subject departs the country. In export cases, where the offense is often non-extraditable, that risk can be fatal to the success of the case.

(7) The Commerce Department is authorized to deny export privileges to a company that has been convicted of violating the Export Administration Act. However, a company shown to be involved in espionage—indeed, a company shown to be a haven for Soviet Bloc spies—cannot be denied export privileges if the corporation or its officers were not convicted of violating the Export Administration Act. That is the interpretation of the law given the subcommittee by Lawrence J. Brady, the Assistant Secretary of Commerce for Trade Administration. Polamco, an Illinois firm owned in part by Poland, was found to have been the base of operations for a Polish spy network that bribed William Holden Bell, a Hughes Aircraft radar specialist. Bell turned over secret military documents to Polish agents. Brady testified that the Commerce Department has no authority to deny Polamco export privileges because a representative of the firm had violated the espionage statute, not the Export Administration Act. The act should be amended so that export privileges would be denied automatically to firms whose owners violated the espionage statute or any other law when the transgression was aimed at the illegal transfer of military or dual-use technology.

(8) The enforcement tools currently available to the U.S. Customs Service should be broadened. Consideration should be given to granting Customs officers express statutory authority for warrantless arrest and search and seizure in cases of outbound cargo and persons,

generally equivalent to that authority which Customs now possesses in cases of inbound cargoes and persons. Express statutory authority would enhance Customs' effectiveness in full enforcement of the export laws. This authority has been implied by the courts in some cases.

(9) The Federal electronic surveillance statutes should be amended to permit court-authorized surveillance where there is probable cause to believe that a violation of either the Export Administration Act or the Arms Export Control Act is being committed. As with the recommendations on Customs' authority, this revision would enhance law enforcement's ability to investigate complex export cases.

(10) Penalties for violation of the Arms Export Control Act should be increased to match those currently available under the Export Administration Act (for entities, a fine of $1,000,000 or five times the value of the exports, whichever is greater; for persons, 10 years imprisonment or a $250,000 fine, or both).

(11) The RICO statute (18 U.S.C. 1962 et seq.) should be amended to include, as predicate offenses in proving racketeering activity, violations of the Export Administration Act. Export violations often have been treated as "minor" offenses, resulting in minimal sentences and the inability to pursue extradition with foreign governments. Prosecution under RICO would expose offenders to a possible 20 year prison sentence and an increased likelihood of extradition.

(12) Volker Nast of Hamburg, Werner J. Bruchhausen of Dusseldorf and Dietmar Ulrichshofer of Vienna have in common the fact that each was indicted in the United States on charges that they conspired to ship militarily critical high technology to the Soviet Union. None of the men was prosecuted, however, because they remained in their native lands free from American justice. In Nast's case, he was indicted twice—in California in 1976, in Maryland in 1981—and, regarding Bruchhausen and Ulrichshofer, their alleged crimes constituted one of the most serious diversions ever perpetrated.

Bringing reported criminals like Nast, Bruchhausen and Ulrichshofer to justice is a difficult task. Most nations are very hesitant to allow extradition of their own citizens. West Germany, for example, has a constitutional prohibition against extradition of German nationals. Moreover, as European law experts have pointed out, criminal sanctions in the German export control system are exceptional, in view of the free trade orientation of German foreign economic relations legislation, and most infractions of it are punishable merely by administrative fines. Similarly, few nations treat export violations as serious offenses, as the United States does.

The subcommittee asked the Library of Congress to evaluate the problem raised by alleged violators like Volker Nast.[8] The Library said:

> It is a well-recognized principle in international law that a State refusing to extradite a criminal should punish him according to its municipal laws. This principle has been expressed in numerous international conventions dealing with the suppression of crimes, and these agreements frequently contain clauses obligating the member countries to make the reprehensive conduct punishable according to their own laws

[8] The Library of Congress study, entitled "Problems of Enforcement of National Security Export Controls Involving Illegal Conduct Abroad," was prepared by Dr. Edith Palmer, Senior Legal Specialist in the European Law Division.

> and to establish jurisdiction in their laws over offenders whose extradition is refused. Whereas these conventions deal with universal crimes for which there is a broad consensus that they need to be suppressed, this may not be the case with regard to U.S. export controls. *However, the protection of these controls might well constitute an obligation among the members of the North Atlantic Treaty to protect their mutual security by adopting laws to enforce these controls.* (Emphasis added.)

The subcommittee concurs with the Library of Congress in the suggestion that one solution to the high technology diversion problem can be found in unified action by the NATO Alliance. The U.S. and its NATO allies are working together to blunt the military threat posed by the Soviet Union and the Warsaw Pact nations. Yet all too often America's European allies seem not to comprehend the connection between their own security and the illegal export of militarily critical technology to the Soviet Union.

It is unlikely that Volker Nast, Werner Bruchhausen and other alleged export control violators living in Western Europe will ever be brought to justice in the United States. In most instances, extradition may be out of the question. But the governments of Western Europe must be made to understand that the issue of high technology diversions to the U.S.S.R. is not merely an American problem. It is a problem for the entire Western world.

In this regard, the subcommittee recommends that the American representatives to NATO take steps to inform more thoroughly the members of the Alliance on the nature of technology diversions and how they undermine the NATO effort. Within the context of NATO, the U.S. and the Allies can devise mutually agreeable procedures for dealing with Soviet surrogates like Volker Nast whose activities pose a threat to each member nation's national security but who, so far, have been immune from prosecution. It should be pointed out to the Allies, for example, that the Microwave Surveillance Receiver system Volker Nast tried to ship from the U.S. to the Soviet Bloc has military applications that can be used against all NATO members, not just the United States.

The U.S. Department of State should followup on the NATO initiatives. In consultation with the Department of Defense, Justice and Treasury, the State Department should meet with the Western Democracies, Japan and with other countries friendly to the West in an effort to negotiate agreements whereby procedures are established providing for prompt and effective prosecution of persons charged with serious export law violations regarding the shipment of militarily critical technology to the Soviet Union.

Testimony at the subcommittee hearings indicated that the Western European and Japanese governments make export policy without guidance from their own defense ministries. The U.S. Defense Department is encouraging these nations to include their own military officials in the writing of export policy and regulations. The Defense Department is to be commended for these efforts. It is an unwise course for any of America's Allies and friends to develop export policy without advice from their own defense ministries. By the same token, inconsistencies between our export policies and those of our

allies can hamper the ability of American businessmen to compete in the international marketplace. We must work with our Allies to develop effective export policies consistent with America's own efforts to promote exports on the one hand, yet control the transfer of sensitive technology on the other.

(13) The region in Santa Clara County, California, popularly known as the "Silicon Valley," the heart of America's growing microprocessor industry, is a prime target of Soviet efforts to transfer sensitive technology. Yet the subcommittee was told that a strong Federal law enforcement presence has been lacking in the Silicon Valley in the past. State enforcement efforts must be supplemented by a Federal interest in the problem. The subcommittee notes assurances from the FBI that it is aware of this problem and is taking steps to increase its presence in the Silicon Valley and other high technology centers. The Bureau is to be commended for its corrective action in this regard.

ROLE OF PRIVATE INDUSTRY

(14) The technology transfer problem is, by all indications, a massive one requiring the attention of both the government and the private sector. Law enforcement and industry spokesmen suggested that many high technology companies remain unaware of the extent of the problem. Reportedly, industry interaction with the Commerce Department is inadequate; unfamiliarity with the lists of controlled exports is common within the industry.

The FBI's DECA (Development of Counterintelligence Awareness) program, aimed at improving the level of communication with the private sector, directly educates companies involved in Defense contracts with the problem of technology transfer. The Defense Department has begun a similar program with the business community. There is a need for similar efforts by other government agencies vested with technology transfer controls to inform companies dealing in sensitive but non-classified technology of their responsibilities in this area.

(15) Private industry must contribute directly to any effort to halt the technology drain. There is a lack of sufficient security precautions at the sources of production in the technology industries. Lax security measures were cited in some Silicon Valley plants. William Bell, a Hughes Aircraft engineer convicted of selling military secrets to Polish spy Marian Zacharski, had access to sensitive information on the basis of a security clearance which had not been reviewed in 28 years. The private sector, through the efforts of individual enterprises and trade and professional associations, should be encouraged to maintain more effective security measures in plants producing sensitive high technology items. Massive Soviet efforts to obtain U.S. technological resources can be countered only through vigorous government and law enforcement efforts, bolstered by the strong support of America's high technology industries.

DEFENSE DEPARTMENT STUDY

(16) In its preliminary investigation, the subcommittee staff found that the Defense Department's role in the export control process has

been affected adversely by fragmentation of key functions and responsibilities. An effective national export control policy must balance the national security interests of DOD, the foreign policy interests of the Department of State and the economic considerations put forward by the Commerce Department. With three Cabinet-level agencies involved, achieving the necessary coordination and cooperation will never be an easy task, even under the best of circumstances. That is why it is essential that the Defense Department formulate a consistent and comprehensive policy, a policy that reflects the harmonious inner-working of the several affected DOD components. If, as the subcommittee staff asserted, there is uncertainty as to which office of DOD is authorized to manage export control questions, the Department cannot make adequate policy in this field; nor will its actions with regard to other government agencies be as effective as they should be. The Secretary of Defense should direct an examination of the Department's procedures and organization regarding technology transfer and export control, and define clearly, with no possibility of ambiguity, where primary responsibilities are to reside. The Secretary may wish to consider the possibility of creating a new office, at an appropriately senior level, whose sole function would be to provide oversight and direction in the Department's technology transfer programs. In his study, the Secretary should make certain that the office which has the function of reviewing export license cases has sufficient permanent resources. The license review process is a vital part of export control. If it is determined that the office needs additional resources, every effort should be made to obtain them. It is a false economy, indeed, to cut back on resources in a function whose work product is so important to the objective of reducing the Soviets' access to American technology.

In addition, the Secretary may want to consider the possible need for improved funding for the Department's research laboratories and facilities which carry out export control duties such as license applications and development of export control lists. A DOD spokesman told the subcommittee that this responsibility should be funded permanently and chartered. In his study, the Secretary also should ascertain that the Defense Department is carrying out effectively its responsibility to oversee government programs which involved visitations to the U.S. of Soviet and Soviet Bloc scientific and technical professionals and students.

FREEDOM OF INFORMATION

(17) The Freedom of Information Act should be amended to eliminate the application of the act to information requests made by foreign nationals. In light of the disclosure of sensitive information to foreign nationals, "cottage" disclosure industries, and others, such statutory revisions would inject a reasonable sense of national security considerations into disclosure practices mandated by the Freedom of Information Act.

In addition, FOIA should be amended by adding a new exemption, one that would exempt requests for technical information relating to items which would otherwise require a validated export license. Language to that effect was included in legislation, S. 1730, to amend

FOIA that was voted out of the Senate Judiciary Committee on May 20, 1982.

The following Senators, who were Members of the Permanent Subcommittee on Investigations at the time of the hearings, have approved this report:

William V. Roth, Jr.
Warren B. Rudman
William S. Cohen [1]
Sam Nunn
Henry M. Jackson
Lawton Chiles
Jim Sasser
John Glenn

The Members of the Committee on Governmental Affairs, except those who were members of the Senate Permanent Subcommittee on Investigations at the time of the hearings, did not sit on the hearings on which the above report was prepared. Under these circumstances, they have taken no part in the preparation and submission of the report except to authorize its filing as a report made by the subcommittee.

---

[1] See p. 68 for additional views of Senator Cohen.

ADDITIONAL VIEWS OF SENATOR WILLIAM S. COHEN

I commend the efforts of Chairman Roth and the Permanent Subcommittee on Investigations for producing this excellent report on technology transfer. The report brings attention to these crucial issues and I agree with most of its recommendations.

I would like the record to reflect, however, the efforts undertaken by the Reagan Administration in the area of technology transfer. President Reagan recognizes the risk associated with a trade policy which allows our adversaries access to our technology and has given a high priority to protecting our technological lead upon which our national security depends.

Since Lawrence Brady assumed his responsibilities as Assistant Secretary of Trade Administration, many important initiatives have been undertaken. These include:

The creation of a Foreign Technical Assessment Center within the Office of Export Administration. This Center will develop and maintain a data base enabling Commerce to assess foreign availability, in conformity with the Export Administration Act. In addition to analyzing foreign availability within the free world, the Center will also be capable of assessing communist held technologies through the increased support of the intelligence community. Such a capability is a crucial first step in the overall enforcement area, particularly in preventive enforcement.

The pursuit of stronger ties and cooperation with the intelligence community and other enforcement agencies. For example, Commerce has been working closely with the U.S. Customs Service in support of Operation Exodus. This information includes the sharing of relevant license information with Customs. For example, there has been established within Commerce a special analytical unit which has developed an innovative intelligence approach that relates the application of link analysis techniques to Commerce's license application files. The analyses produced by this unit are reported to have been extremely effective in identifying firms engaged in diverting critical technology to the Soviet Union as well as her client states and in pinpointing new diversion routes. In addition, Commerce is in the process of developing agreements with other law enforcement and intelligence agencies which would facilitate the exchange of appropriate information so as to benefit this country's overall export control program.

The elevation to Office status of the Compliance Division. Together with the Office of Antiboycott Enforcement, the Office of Export Enforcement will comprise a new aggressive enforcement organization to be headed by a new Deputy Assistant Secretary for Export Enforcement.

The designation of Theodore W. Wu, formerly an Assistant U.S. Attorney for the Central District of California, to fill the new Deputy

Assistant Secretary position. Mr. Wu has an extraordinary record in export control, having successfully investigated and prosecuted some of the U.S.'s most notorious export diversion and arms export control cases, and is highly regarded by the law enforcement and national security communities.

The planned establishment of new field offices in San Francisco and Los Angeles. These cities were strategically chosen because of the large number of high technology industries located in their vacinities which are targeted by hostile intelligence services. The new field offices represent a 40-percent increase in Commerce's enforcement resources, and will be an important supplement to the Washington Headquarters and New York Field Office.

The formulation of an in-house training program for Commerce Export Enforcement special agents. This training program will include instruction not only in conventional law enforcement, such as surveillance techniques, search and seizure, arrest and weapon skills, but also in export control enforcement techniques and trade intelligence and technology acquisition trend analysis.

Once again, I would like to commend the initiatives that have been undertaken by this Administration to prevent the flow of strategic technology to Eastern Bloc countries. I do, however, believe that more drastic steps are needed to address this issue and for this reason I have cosponsored the Office of Strategic Trade Act of 1982. As many of my colleagues are aware, this legislation would establish an office independent of the Commerce Department to carry out the functions of the Export Administration Act.

I look forward to working with the Administration to produce a meaningful export administration policy.

○